

COMPETENCIA DIGITAL II

PROFESORA: BELÉN TORRECILLA

Fraude en Internet

1. Recomendaciones
2. Algunas tiendas recomendadas
3. JUEGO: ¿Verdad o Fraude?
 - *Mensajes*
 - *WhatsApps*
 - *Correos*

VIDEO: ¿Cuáles son los riesgos de Internet?

RTVE PLAY - LOS RIESGOS DE INTERNET

<https://www.rtve.es/play/videos/programa/cuales-son-riesgos-internet-como-p-revenirlos/6825859/>



VIDEO: Ciberseguridad para todos

OFICINA DE SEGURIDAD DEL INTERNAUTA

https://youtu.be/bv-h_omPJog?si=JJMv1oBayGleZ_je

ENLACE WEB INCIBE (Instituto Nacional de Ciberseguridad:

<https://www.incibe.es/ciudadania/experiencia-senior>

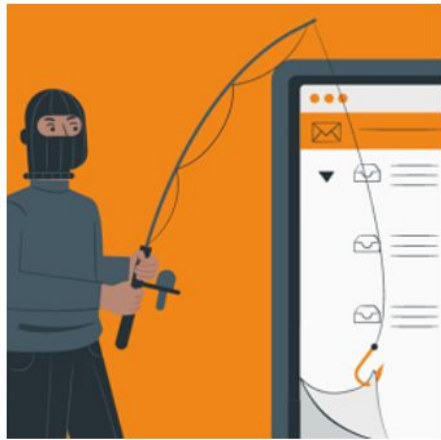
El auge del fraude en Internet

- La **ingeniería social y los fraudes online** son cada vez más comunes en la era digital en la que vivimos. Los ciberdelincuentes utilizan diversas técnicas para robar información personal o financiera, instalar programas maliciosos o tomar el control de los dispositivos.



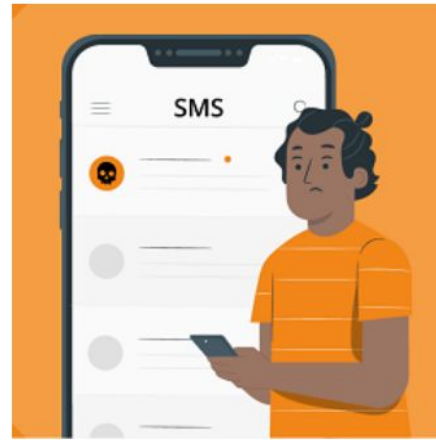
Tipos de Phishing

- Técnicas utilizadas para engañar a las personas y obtener información personal, como contraseñas y números de tarjetas de crédito a través de correos electrónicos, SMS o llamadas telefónicas. Para ello, suele suplantar a entidades o empresas conocidas y utilizar temas que apelan a las emociones de las víctimas para conseguir su objetivo.



Phishing (Campaña)

Se trata de una técnica utilizada por ciberdelincuentes para obtener información confidencial como contraseñas, números de tarjetas de crédito y otra información de carácter personal de los usuarios a través del envío de correos electrónicos fraudulentos.



Smishing (Campaña)

El *smishing* es un término que se utiliza para describir una forma de fraude en la que los delincuentes intentan engañar a las personas para que divulguen información personal o financiera enviándoles mensajes de texto (SMS) que incorporan enlaces fraudulentos.



Vishing (Campaña)

El *vishing* es una técnica de ingeniería social utilizada por los ciberdelincuentes para engañar a los usuarios a través de llamadas de teléfono fraudulentas y obtener así información personal sobre ellos, guiarles para que descarguen e instalen programas maliciosos, así como intentar que realicen algún pago bajo algún pretexto.

Phishing: Correo y Web

■ ¿Qué es el “phishing”?

La palabra “**phishing**” viene del inglés *fishing*, que significa “**pescar**”. En este caso, los delincuentes “pescan” personas para robarles información.



■ ¿Cómo lo hacen?

Envían **correos electrónicos falsos** o crean **páginas web falsas** que parecen de bancos, tiendas o servicios conocidos.

El objetivo es que la persona **escriba sus datos personales**, como contraseñas o números de tarjeta, pensando que está en un sitio seguro.

■ Cómo protegerse:

- X No hagas clic en enlaces de correos sospechosos.
- X Comprueba que la dirección web sea la oficial (empiece con “https” y tenga el nombre correcto).
- X Si dudas, llama directamente a la empresa antes de responder.

Smishing y Whising

■ ¿Qué es el “smishing”?

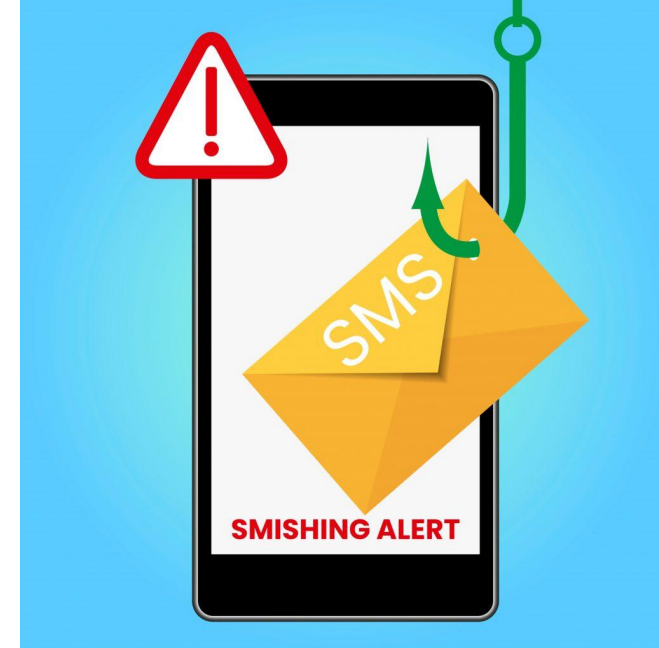
La palabra “smishing” viene de **SMS** (mensaje de texto) y phishing (“pescar” en inglés). Significa que los delincuentes envían mensajes falsos al móvil para engañar a las personas y robar sus datos o dinero.

■ ¿Wishing o el “WhatsApp phishing”?

Es **el mismo tipo de engaño**, pero **por WhatsApp**.

Los delincuentes envían mensajes que parecen venir de una empresa, un amigo o un familiar, para que **pinches en un enlace o compartas información**.

- X No abras enlaces que te parezcan raros, aunque vengan de alguien conocido.
- X No des tus datos personales ni contraseñas por mensajes.
- X Si tienes dudas, llama tú directamente a la persona o empresa para comprobarlo.



Vishing

■ ¿Qué es el “vishing”?

La palabra “**vishing**” viene de voice (**voz**, en inglés) y phishing (“pescar”). Significa que los delincuentes usan llamadas telefónicas para engañar y robar información personal o dinero.

En realidad, no es el banco o tu compañía de teléfono, sino un estafador que intenta que la persona le dé sus datos.



- X Desconfía de llamadas que pidan contraseñas, números de cuenta o datos personales.
- X No devuelvas llamadas a números desconocidos o sospechosos.
- X Si dicen ser de tu banco u otra empresa, cuelga y llama tú mismo al número oficial.

Qrshing

■ ¿Qué es el “vishing”?

La palabra “QRshing” viene de **QR** (el código cuadrado que se escanea con el móvil) y phishing (“pescar”, en inglés).

Es una forma de engaño a través de códigos QR falsos.



Los delincuentes colocan códigos QR engañosos en carteles, mesas de restaurantes o incluso sobre otros códigos verdaderos.

Cuando alguien los escanea, el código lleva a una página falsa que pide datos personales o instala un programa malicioso en el teléfono.

- X No abras enlaces que te parezcan raros, aunque vengan de alguien conocido.
- X No des tus datos personales ni contraseñas por mensajes.
- X Si tienes dudas, llama tú directamente a la persona o empresa para comprobarlo.

Ejemplo Phishing (Correo)

limitación de cuenta

Bankia SA <contact246847@webmail.indra.es> 2018 12:26 (hace 3 días)

para

inglés > español Traducir mensaje Desactivar para: inglés x

Bankia

Buenos días,

Necesitamos actualizar su información para cumplir con la ley 11/2018 sobre prevención. Actualizar la seguridad contra ataques a la cuenta. Solo tejdaremos unos minutos. El formulario de conocimiento del cliente ahora está actualizado.

Se pone en línea una nueva aplicación de seguridad "**BANKIA SECURE**" para proteger sus dispositivos Android contra ataques fraudulentos.

Actualícelos ahora, o lo antes posible desde la sección de 'Datos Personales' de tu perfil.

Es importante que lo actualizas en un plazo máximo de 8 días. En caso contrario, recuerda que tu operativa en la web y en la app está limitada a consultas, por teléfono puedes seguir operando, pero tus cuentas no podrán admitir nuevos ingresos hasta que estén actualizados. Gracias por tu colaboración.

Bankia S.A.

Note: Por favor, no responda este mail. El mensaje fue generado en forma automática.

RE: aviso de seguridad. - Mensaje (HTML)

Archivo Mensaje Ayuda ¿Qué desea hacer?

Ignorar Eliminar Archivo Responder Responder a todos Reenviar Más

Eliminar Responder Pasos rápidos

RE: aviso de seguridad.

ING <oficinas-num-39022@eircom.net>
Para ING Banco | Particulares

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes.

Seguridad-ING.pdf
455 KB

ING DIRECT

Aviso Importante :

Estimado cliente ,

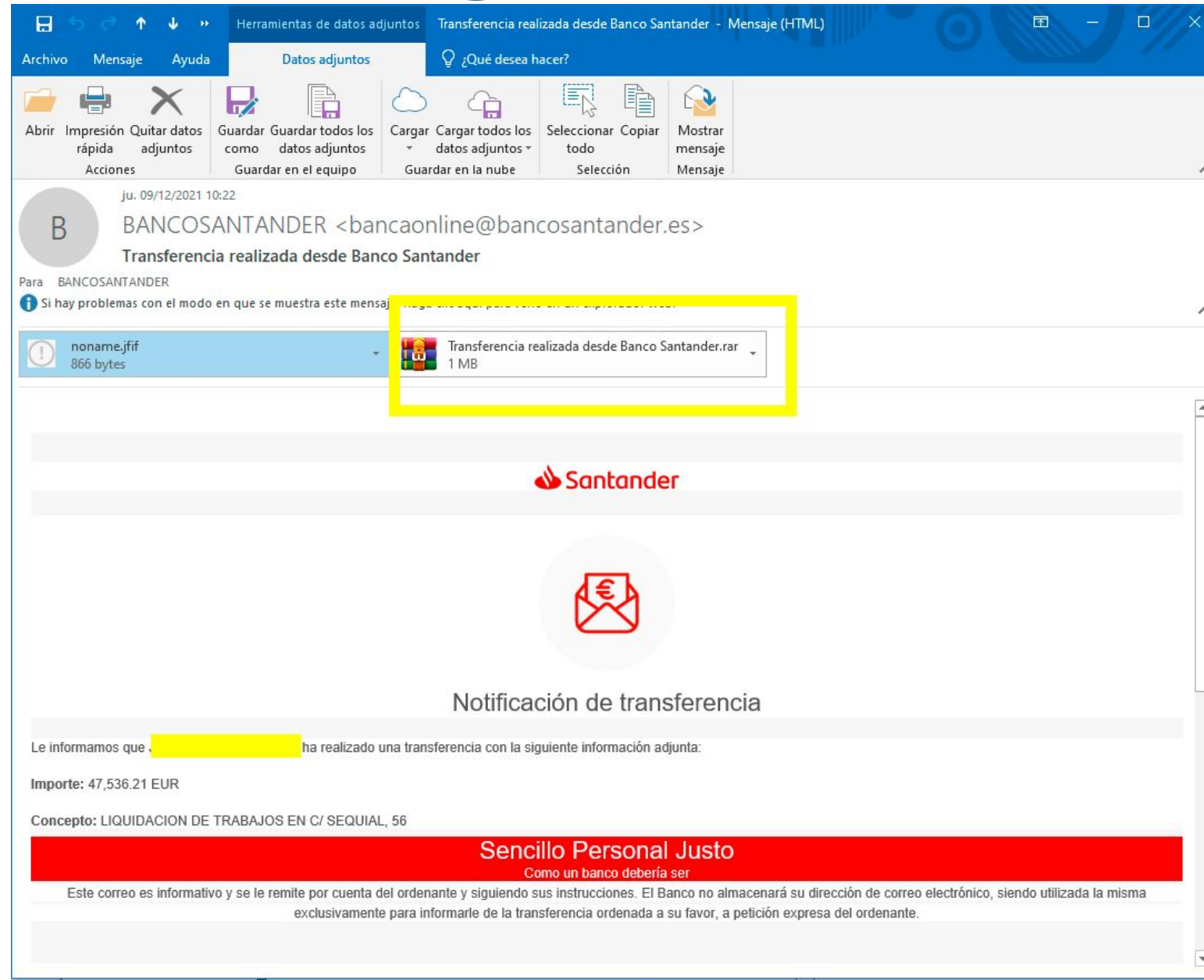
Para evitar el uso fraudulento de tarjetas de crédito en internet ,
ING tiene un nuevo sistema de control:

[iniciar sesion en su cuenta](#)

ING Banco Online © 2021

Servicio personalizado todos los dias .

Ejemplo Phishing (Correo)



Ejemplo Phishing (Correo)

Windows Live™ Hotmail (999+) Messenger SkyDrive | MSN

Hotmail Nuevo | Responder Responder a todos Reenviar | Eliminar Correo no deseado Limpiar ▾ Marcar como ▾ Mover a ▾ Categorías ▾ |

Entrada (153!)

Felicitaciones, usted ganó 200 Volver a mensajes |

ganadores@bbva.es [Agregar a contactos](#) 11:18 a.m.
Responder ▾

BBVA

Felicidades,

Usted es uno de los 400 ganadores del premio por valor de 200 € a fecha de 17 de enero de 2012.
Para obtener el premio, haga clic en el enlace más abajo para su concesión.
Su premio será abonado a su cuenta de BBVA en las próximas 24 horas.

Haga clic en el enlace de abajo para continuar:
<http://www.bbva.es/ganadores>

Gracias

Banco Bilbao Vizcaya Argentaria S.A. - 2012

Página principal | Nuevo | Responder Responder a todos Reenviar | Eliminar Correo no deseado Limpiar ▾ Marcar como ▾ Mover a ▾ Categorías ▾ |

Contactos
Calendario

Missing Plug-in

bbva.24.org.es/wp-include/

Phishing

Spam Loco

Ejemplo Smising (Banco)

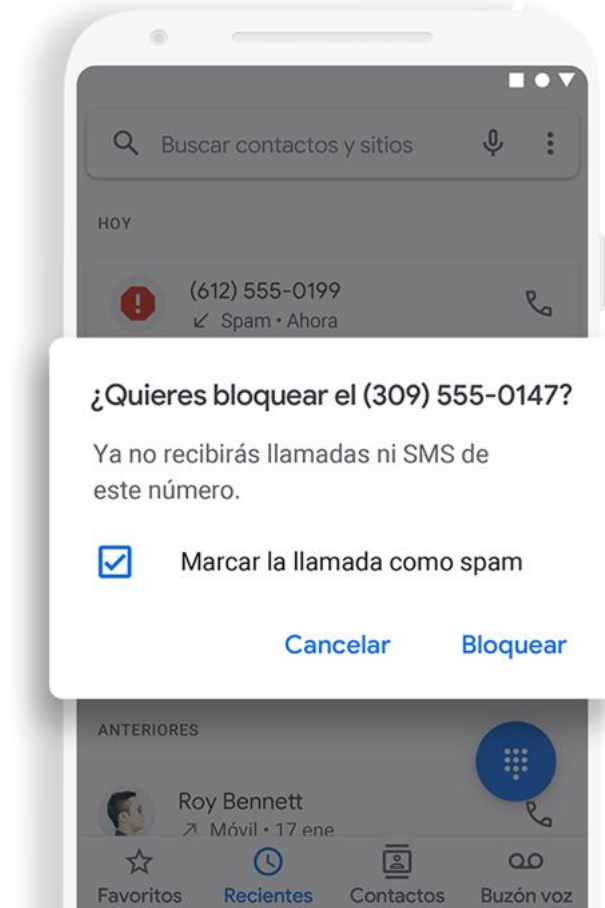
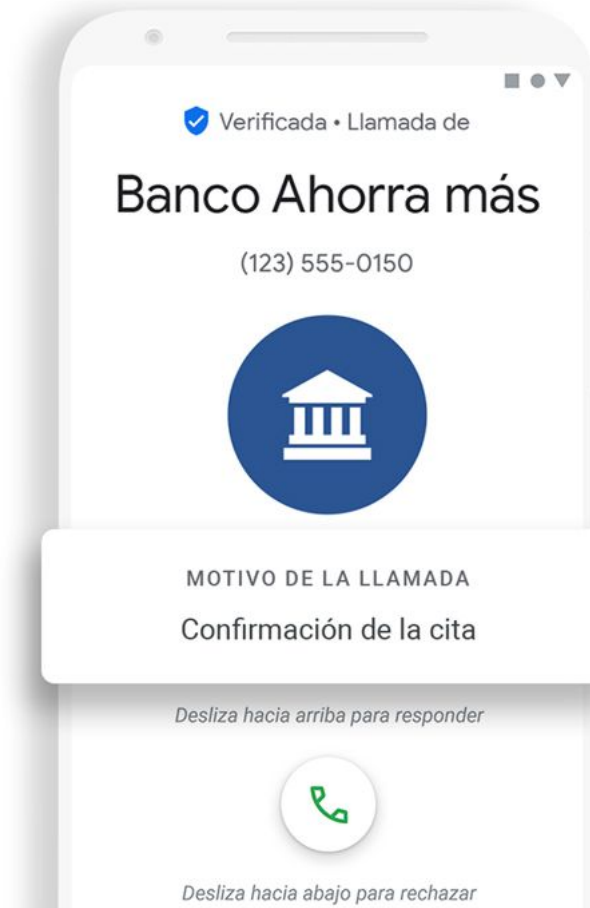
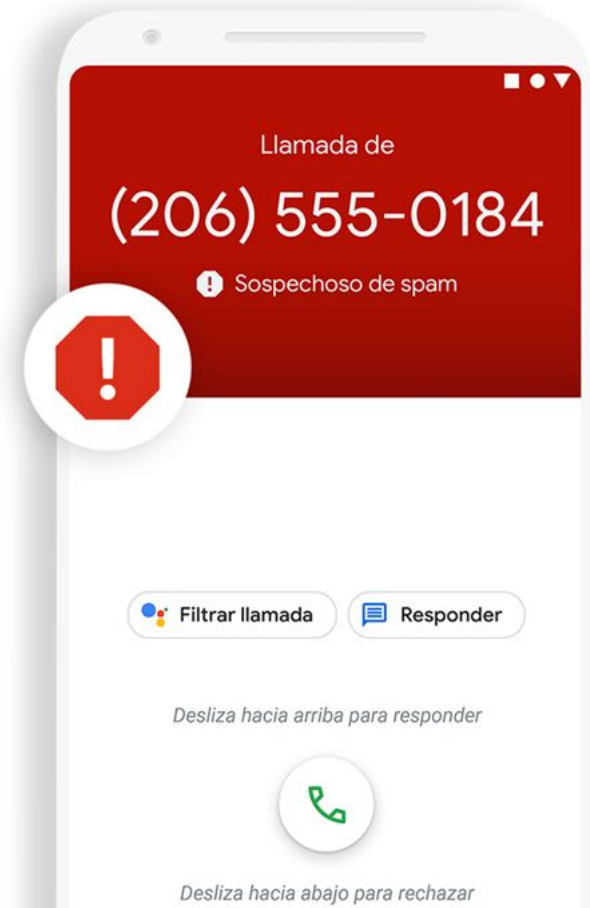
miércoles, 24 ago • 17:38

Mensaje de texto a 664 18 57 10 (SMS/MMS)



SANTANDER: Su tarjeta bancaria ha sido bloqueada temporalmente. Para activar su cuenta, puede acceder de forma segura desde: <https://s.id/1fBaM>

Ejemplo Vising (Llamadas)



Ejemplo Quising (Códigos QR)



Recomendaciones previas

- **LEER** antes de pinchar en algo o antes de introducir nuestros datos.
- Utilizar la Autenticación/Verificación en 2 pasos para cuentas importantes (Google, WhatsApp, Facebook...)
- Al hacer comprar online, utilizar una tarjeta prepago/monedero/virtual.
- No conectarse a redes WiFi abiertas.
- Infórmate y lee reseñas sobre la tienda virtual antes de comprar
- No facilites ningún dato personal en plataformas online o redes sociales.
- Mantén actualizado tu smartphone/ordenador
- Utilizar contraseñas complejas y seguras, y no tenerlas apuntadas a la vista de cualquiera
- **LEER Y APRENDER** a detectar posibles correos / mensajes / llamadas maliciosas

IMPORTANTE TAMBIÉN

NO LE TENGÁIS MIEDO A INTERNET

Sí hay que ser precavidos. Pero no debemos huir de la tecnología sino aprender a utilizarla y entenderla.



VERDAD

FRAUDE

JUEGO: ¿VERDAD O FRAUDE?

En este juego pondrás a prueba tu habilidad para detectar engaños en internet. Verás una serie de **capturas de correos electrónicos y mensajes de texto (SMS)**. Tu misión es **analizar cada uno cuidadosamente** y decidir si se trata de un **mensaje legítimo** o de un **intento de fraude por internet (phishing)**.

Presta atención a los **detalles sospechosos**:

- Direcciones de correo o enlaces extraños
- Errores ortográficos o de formato
- Solicitudes urgentes o poco comunes de información personal
- Mensajes que prometen premios o amenazan con consecuencias

Tu objetivo es **identificar correctamente los fraudes y no caer en las trampas digitales**.

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Correos españa [redacted]@bradfordskips.com>

Carta Certificada CD 61278791640



Su paquete ha llegado a 30 de agosto de 2016. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.



CD 61278791640

[Descargar información sobre su envío](#)

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



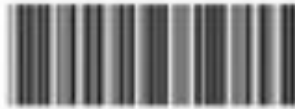
Correos españa [redacted]@bradfordskips.com>

Carta Certificada CD 61278791640



 **CORREOS**

Su paquete ha llegado a 30 de agosto de 2016. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.



CD 61278791640

[Descargar información sobre su envío](#)

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Responder Reenviar Archivar No deseado Eliminar Más

De Online Bbva.es <info@graexcon.com> ☆

Asunto Bbva(es): verifique su cuenta introduciendo... 29/07/2019 18:39

A undisclosed-recipients; ☆

BBVA

Hola, su cuenta en línea ha sido suspendida temporalmente.

Necesitamos que verifique su cuenta introduciendo sus credenciales y SMS verificación .

Asegurese de introducir sus datos correctamente y su numero de telefono esta cerca de usted para verificar su identidad por el telefono adormecer: .

- 1- Acceder a mi
- 2- Ingrese el codigo de verificacion de SMS en la pagina de verificacion
- 3- inicie sesion y siga los pasos haciendo clic a continuacion:

[Acceder a mi](#)

Nota: Si usted no activa su cuenta en el próximo 24Hours usted será suspendido de nuestros servicios bancarios.

BBVA Espana Merchant Services, Entidad de Pago S.L.U., Calle Isla Graciosa 5, 28703 San Sebastián de los Reyes, Madrid, Espana.

<http://fortyone.web.id/dist/re/>

Responder

De Online Bbva.es <info@graexcon.com> ☆

Asunto Bbva(es): verifique su cuenta introduciendo...

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Responder Reenviar Archivar No deseado Eliminar Más

De Online Bbva.es <info@graexcon.com> ☆

Asunto Bbva(es): verifique su cuenta introduciendo... 29/07/2019 18:39

A undisclosed-recipients; ☆

BBVA

Hola, su cuenta en línea ha sido suspendida temporalmente.

Necesitamos que verifique su cuenta introduciendo sus credenciales y SMS verificación .

Asegurese de introducir sus datos correctamente y su numero de telefono esta cerca de usted para verificar su identidad por el telefono adormecer: .

- 1- Acceder a mi
- 2- Ingrese el codigo de verificacion de SMS en la pagina de verificacion
- 3- inicie sesion y siga los pasos haciendo clic a continuacion:

[Acceder a mi](#)

Nota: Si usted no activa su cuenta en el próximo 24Hours usted será suspendido de nuestros servicios bancarios.

BBVA Espana Merchant Services, Entidad de Pago S.L.U., Calle Isla Graciosa 5, 28703 San Sebastián de los Reyes, Madrid, Espana.

<http://fortyone.web.id/dist/re/>

Responder

De Online Bbva.es <info@graexcon.com> ☆

Asunto Bbva(es): verifique su cuenta introduciendo...

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Aquí tienes el ticket digital del cajero  Recibidos x



Santander Informa <SantanderInforma@emailing.bancosantander-mail.es>
para mí ▼

Si no visualizas correctamente este email haz click [aquí](#)

Este email es para ti, [REDACTED]



Hola [REDACTED],

has realizado una retirada de efectivo de 110,00 EUR en el cajero 0049.1847.10 situado en Poligono Industrial Campollano, Calle G" Modulo 37", Albacete, 02001, Albacete.

Te adjuntamos tu ticket digital. Recuerda que puedes ver tu ticket en la app o en la web.



RETIRADA DE EFECTIVO

CAJERO: 0049.1847.10

FECHA: 03/10/2025

HORA: 20:13

OPERACIÓN: 7941

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Aquí tienes el ticket digital del cajero Recibidos x



Santander Informa <SantanderInforma@emailing.bancosantander-mail.es>
para mí ▼

Si no visualizas correctamente este email haz click [aquí](#)
Este email es para ti, [REDACTED]



Hola [REDACTED],
has realizado una retirada de efectivo de 110,00 EUR en el cajero 0049.1847.10 situado
en Poligono Industrial Campollano, Calle G" Modulo 37", Albacete, 02001, Albacete.

Te adjuntamos tu ticket digital. Recuerda que puedes ver tu ticket en la app o en la
web.



RETIRADA DE EFECTIVO

CAJERO: 0049.1847.10
FECHA: 03/10/2025
HORA: 20:13
OPERACIÓN: 7041



Santander Informa <SantanderInforma@emailing.bancosantander-mail.es>
para mí ▼

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Alerta de seguridad  Recibidos x



Google <no-reply@accounts.google.com>
para mí ▼

vie, 5 sept, 9:55



Nuevo inicio de sesión en Windows



belentorrecilla0@gmail.com

Hemos detectado un nuevo inicio de sesión en tu cuenta de Google en un dispositivo Windows. Si has sido tú, no es necesario que hagas nada. De lo contrario, te ayudaremos a proteger la cuenta.

Comprobar actividad

También puedes ver toda la actividad de seguridad en
<https://myaccount.google.com/notifications>



Google <no-reply@accounts.google.com>
para mí ▼

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Alerta de seguridad  Recibidos x



Google <no-reply@accounts.google.com>
para mí ▼

vie, 5 sept, 9:55



Nuevo inicio de sesión en Windows



belentorrecilla0@gmail.com

Hemos detectado un nuevo inicio de sesión en tu cuenta de Google en un dispositivo Windows. Si has sido tú, no es necesario que hagas nada. De lo contrario, te ayudaremos a proteger la cuenta.

Comprobar actividad

También puedes ver toda la actividad de seguridad en
<https://myaccount.google.com/notifications>

VIDEO: Timo del falso de paquete de correos

<https://www.youtube.com/watch?v=M02GJv1SfhE>

<https://www.rtve.es/play/videos/la-hora-de-la-1/timo-del-falso-paquete-correos/6899125/>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Mensaje de texto
hoy, 15:44

CORREOS: Su paquete no se puede entregar debido a que no se han pagado las tasas de aduana (2,64 €), por favor confirme su pago para evitar retrasos: https://cutt.ly/Siguientes_certificados

JUEGO: ¿VERDAD O FRAUDE?



Mensaje de texto
hoy, 15:44

CORREOS: Su paquete no se puede entregar debido a que no se han pagado las tasas de aduana (2,64 €), por favor confirme su pago para evitar retrasos: https://cutt.ly/Siguientes_certificados

VERDAD

FRAUDE

¿Dónde está el número de seguimiento de nuestro paquete?

¿Qué clase de enlace es <https://cutt.ly> si la empresa debería ser <https://correos.es>?

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

< Correos ELIMINAR

martes, 15 de octubre de 2019

 Estimado cliente, su paquete no se ha podido entregar el 11/10 porque no se han pagado las tasas de aduana (€ 1). Siga las instrucciones: <http://a8n.me/uS2js> 14:02

CORREOS : Estimado, cliente su paquete ha sido retenido por aduanas. Para el envío pague las tasas de (2,64€) accediendo al enlace: [http://a8n.me/uS2js](#)

SERVICIO CORREOS:
Su paquete esta listo para la entrega confirme el pago de aduanas de (1,79 €) en el siguiente enlace: [http://a8n.me/uS2js](#)

Correos Express,
su paquete sigue retenido en aduanas por impago de las tasas (2,64€) puede pagarlos en el siguiente enlace: <https://itsssl.com/vEMEF>

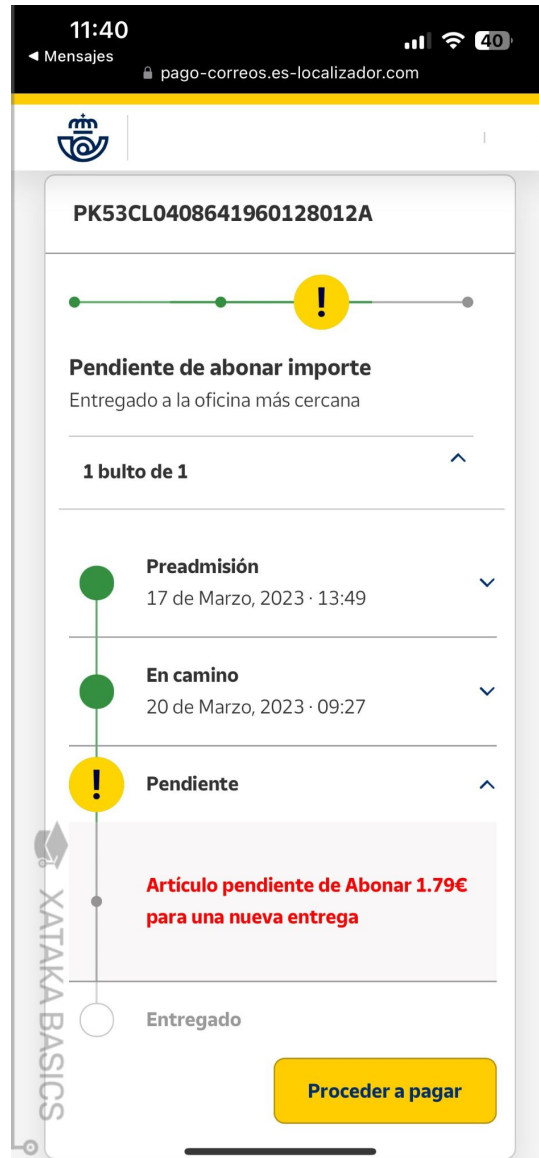
Recibirá su envío de Correos. Los cargos de gestión AEAT son 2,39€. Confirme el pago para continuar con el proceso de entrega: [http://a8n.me/uS2js](#)

[CORREOS] Estimado cliente: Su paquete no se ha podido entregar el 17/11 porque no se han pagado las tasas de aduana (2.64€): Siga las instrucciones : [http://a8n.me/uS2js](#)

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Estas páginas trataran de que pongamos nuestros datos en una web clonada y robarnos la informacion/dinero

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Su envío 0078530078530104738072
no ha sido entregado.Nueva entrega
dia siguiente habil.Cambiar entrega
<https://app.cttexpress.com/m/d.asp?k=HUE2Pt@GPiOY>

jueves, 13 jul • 17:51

Su envío 0078530078530104738072
no ha sido entregado.Nueva entrega
dia siguiente habil.Cambiar entrega
<https://app.cttexpress.com/m/d.asp?k=HUE2Pt@GPiOY>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Su envío 0078530078530104738072
no ha sido entregado.Nueva entrega
dia siguiente habil.Cambiar entrega
<https://app.cttexpress.com/m/d.asp?k=HUE2Pt@GPiOY>

jueves, 13 jul • 17:51

Su envío 0078530078530104738072
no ha sido entregado.Nueva entrega
dia siguiente habil.Cambiar entrega
<https://app.cttexpress.com/m/d.asp?k=HUE2Pt@GPiOY>

Sí nos aparece el numero
de pedido y el enlace nos
lleva a su empresa
“cttexpress.com”

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

←  MRWes

miércoles, 10 de abr de 2019 • 19:07

MRW INFORMA: recibira envio
038223598491 ECOM19 de REPUBLICA
GRAFICA, S.L. EL 11/04/2019. Puede
cambiar fecha entrega en mrw.es/
tr.asp?ta=7734611

19:07

miércoles, 10 de abr de 2019 • 19:07

MRW INFORMA: recibira envio
038223598491 ECOM19 de REPUBLICA
GRAFICA, S.L. EL 11/04/2019. Puede
cambiar fecha entrega en mrw.es/
tr.asp?ta=7734611

19:07

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Sí nos aparece el numero de pedido y el enlace nos lleva a su empresa “mrw.es”

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



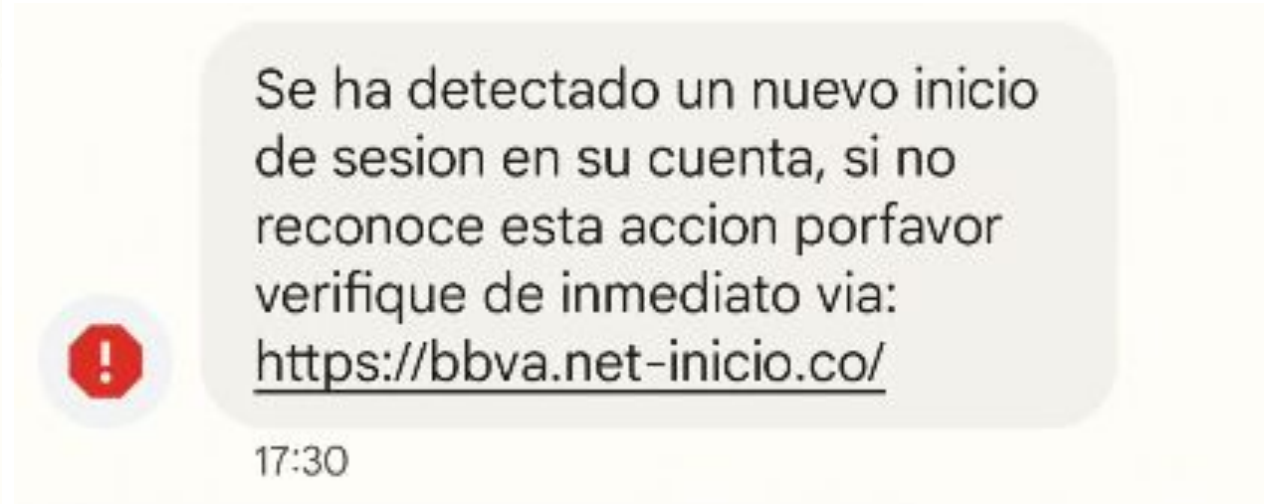
Se ha detectado un nuevo inicio de sesion en su cuenta, si no reconoce esta accion porfavor verifique de inmediato via: <https://bbva.net-inicio.co/>

17:30

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Ya el movil nos está avisando pero además esa no es la web del BBVA

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

18:20    B.  ...

  90 



santander



Resultados encontrados: 3/3



jueves, 19 de may de 2022 • 18:41

Santander: NO COMPARTA ESTE
CODIGO CON NADIE: el codigo para
el registro del dispositivo seguro es
G897G450

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Esto sera verdad solo si acabamos de realizar una transferencia o solicitado algo en ese mismo momento

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

miércoles, 24 ago • 17:38

Mensaje de texto a 664 18 57 10 (SMS/MMS)



SANTANDER: Su tarjeta bancaria ha sido bloqueada temporalmente. Para activar su cuenta, puede acceder de forma segura desde: <https://s.id/1fBaM>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

miércoles, 24 ago • 17:38

Mensaje de texto a 664 18 57 10 (SMS/MMS)



SANTANDER: Su tarjeta bancaria ha sido bloqueada temporalmente. Para activar su cuenta, puede acceder de forma segura desde: <https://s.id/1fBaM>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Apartir del 19 06 no puedes utilizar su cuenta. Tienes que activar el nuevo sistema de seguridad web . Activa ahora: <https://bbva.es-4456.info/b?56694?>



Toca para cargar la vista previa

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Apartir del 19 06 no puedes utilizar su cuenta. Tienes que activar el nuevo sistema de seguridad web . Activa ahora: <https://bbva.es-4456.info/b?56694?>



Toca para cargar la vista previa

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

domingo • 12:42

Acceso no autorizado en su cuenta online. Si no reconoce este acceso verifique inmediatamente: <https://bbva.app-seguridad-web.ru/>



Cargar la vista previa

Se ha intentado realizar un cargo de 490,00 EUR en su cuenta. Si no reconoce esta actividad, verifique inmediatamente: <https://es.bbva-web-alertas.com/>

8:38

97%

Santander

domingo, 21 de agosto

Su cuenta ha sido bloqueada temporalmente por razones de seguridad, para reactivarla verifique en: <https://santander.es-gestion.gq/>

14:10

11

+52 (221) 152 0724 >

Text Message
Monday 12:46 PM

DEBIDO A UN ERROR EN TU TARJETA4***** DEBES ACTUALIZAR TUS ALERTAS EN realiza-tu-altabbv4.info/2



GSAN

Mensaje de texto
hoy, 18:36

Le informamos que ha recibido una orden de transferencia que necesita su atencion. Por tu seguridad acceda a la cuenta online en el sitio www.santandergrupo.es

Mensaje de texto
hoy, 01:23

Alerta ViaBCP
Tienes una transferencia retenida, para activar tus operaciones y evitar el bloqueo de sus cuentas ingrese aqui: <https://bit.ly/Bcp-Retencion>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



INFO: Su cuenta será inhabilitada debido a un inicio de sesión sospechoso. Verifique su dispositivo únicamente desde el siguiente enlace: <https://is.gd/UL6fcx>

13:23

Hola, en relacion con la pandemia COVID19, el Estado destina 350-700 euros a sus ciudadanos.
[https://\[redacted\]20.es](https://[redacted]20.es)

10:55

Escribiéndote con 22623436241 (SMS/MMS)

Hola mama ahora he cambiado de telefono y proveedor. Este es mi numero. Escíbime un whatsapp <https://wa.me/+34623436241>

10:55



Mensaje de texto



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

WhatsApp, puede leerlos ni escucharlos. Toca para obtener más información.

Hola Mamá.

Mi otro teléfono está roto.
este es el nuevo número que puedes
guardar. ❤️👍

Estas en casa?

19:27

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

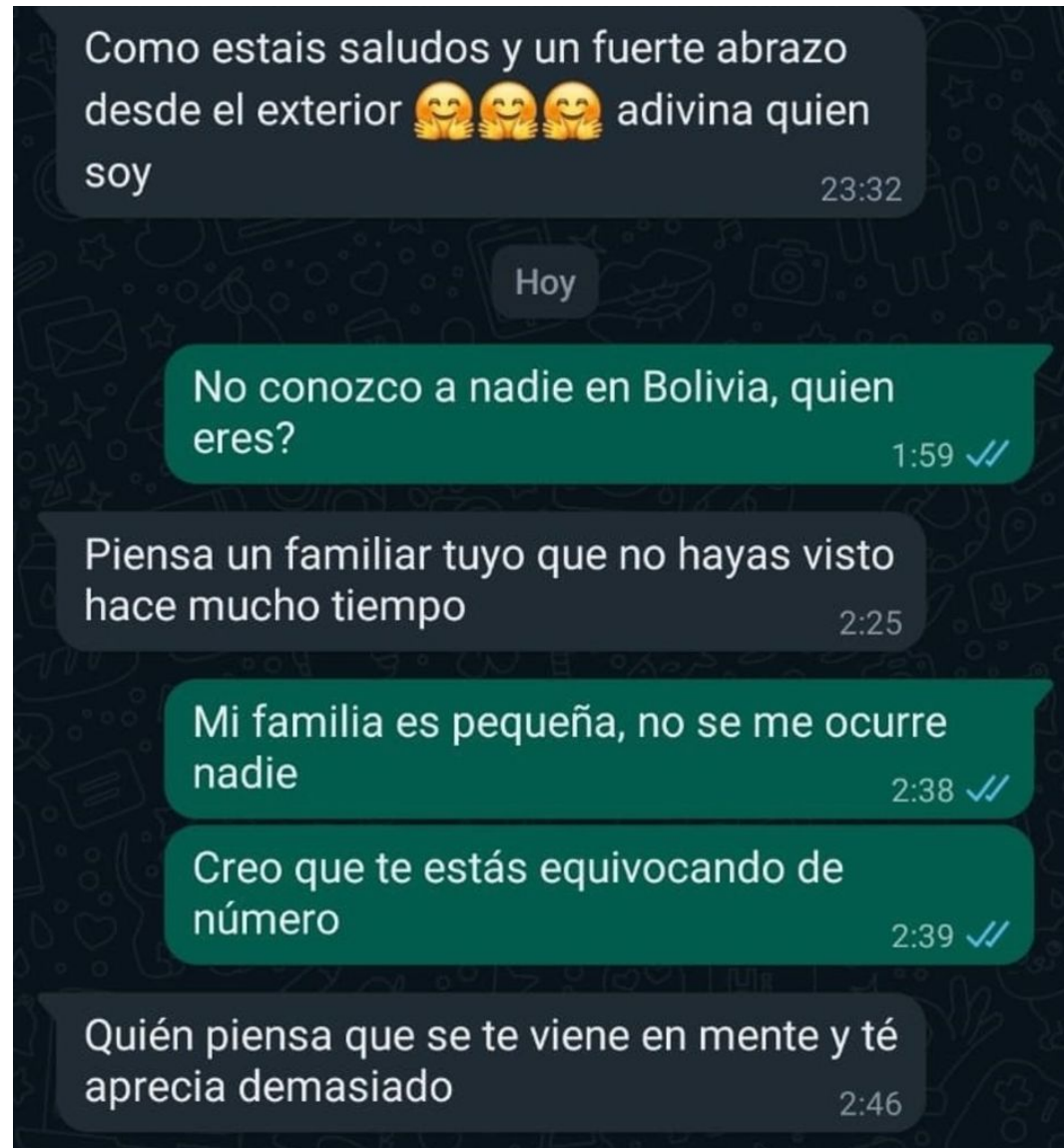
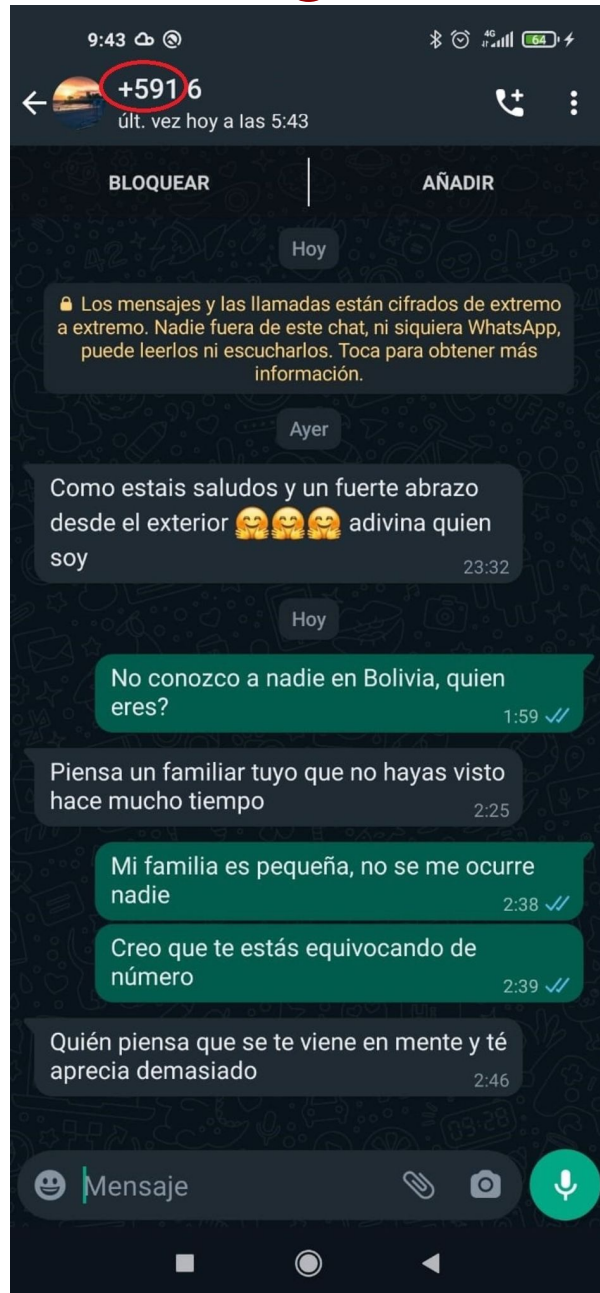
FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

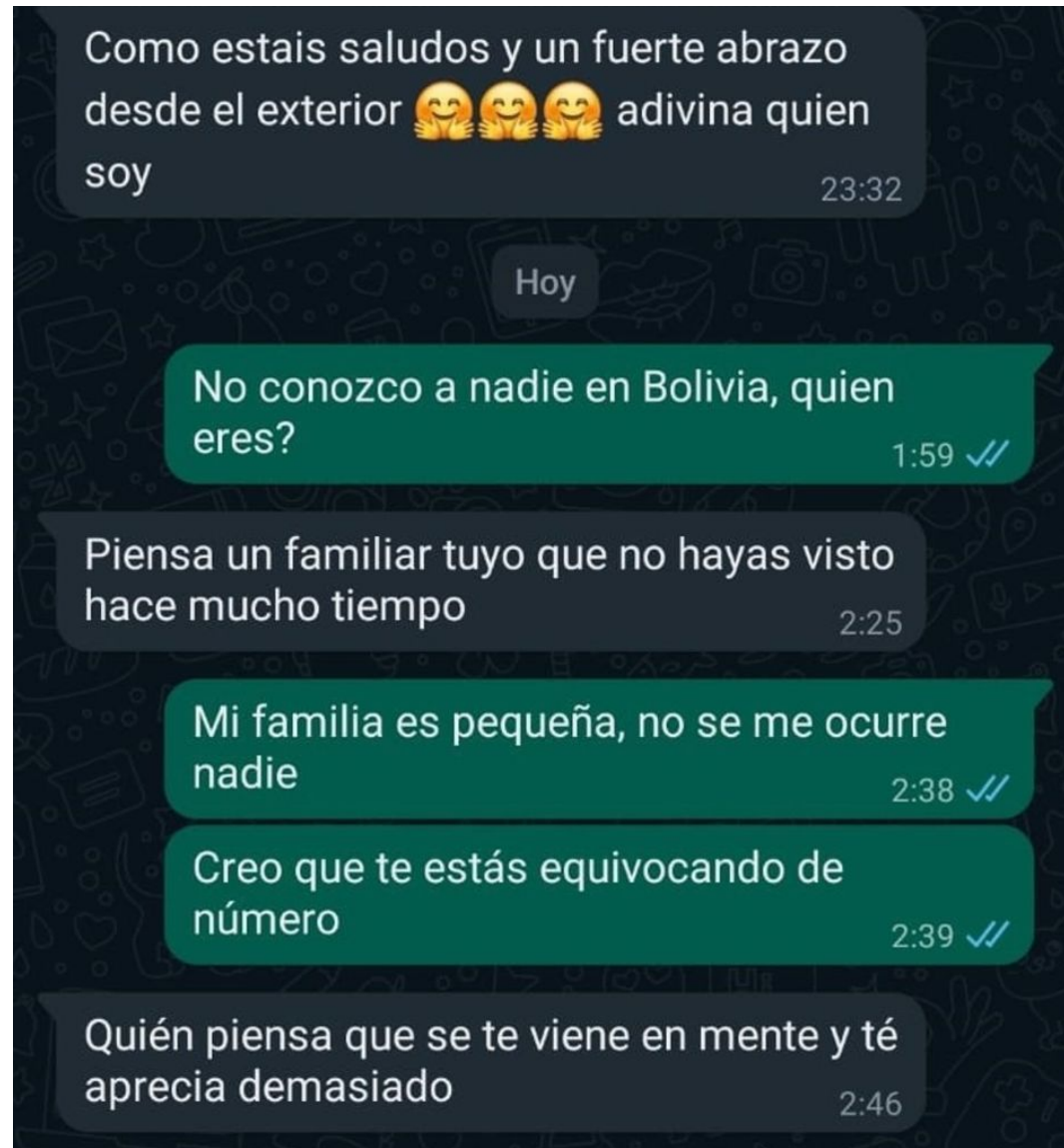
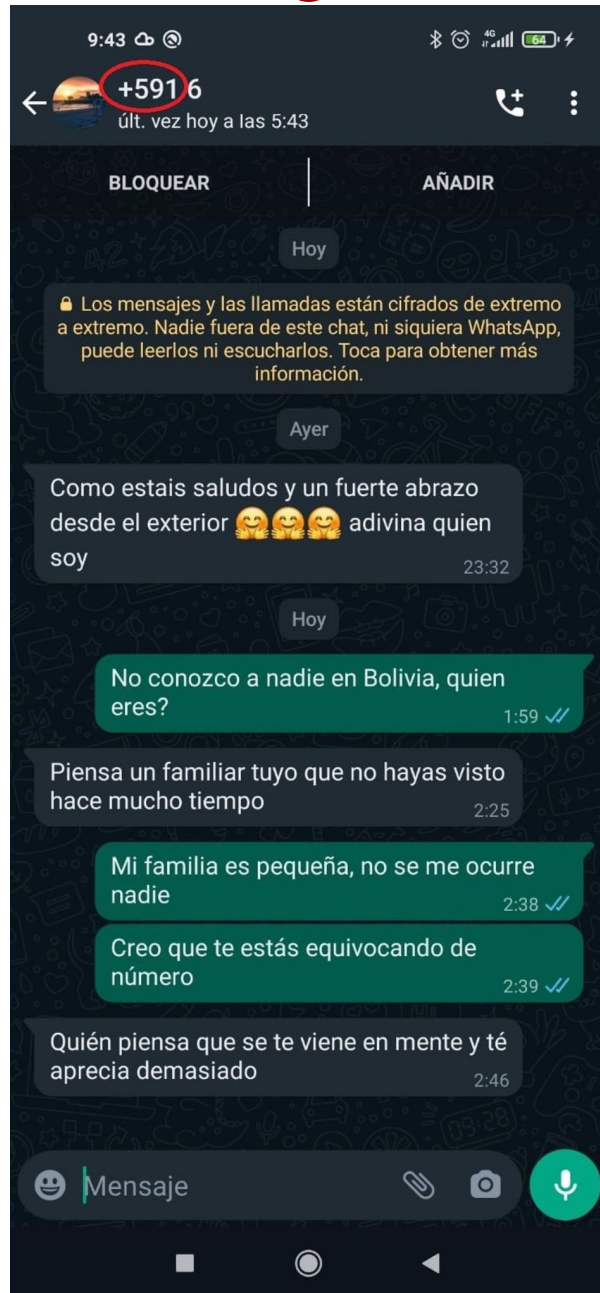
FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

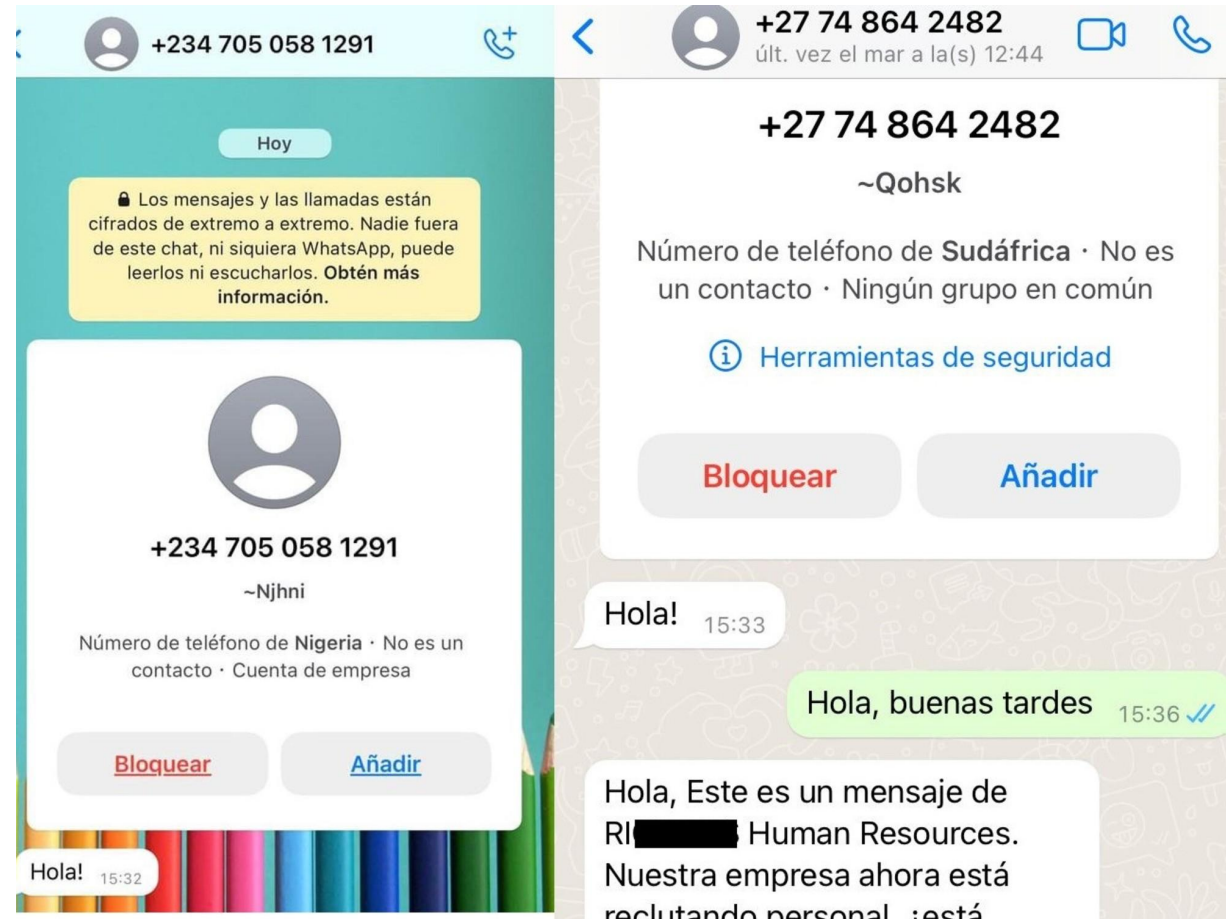
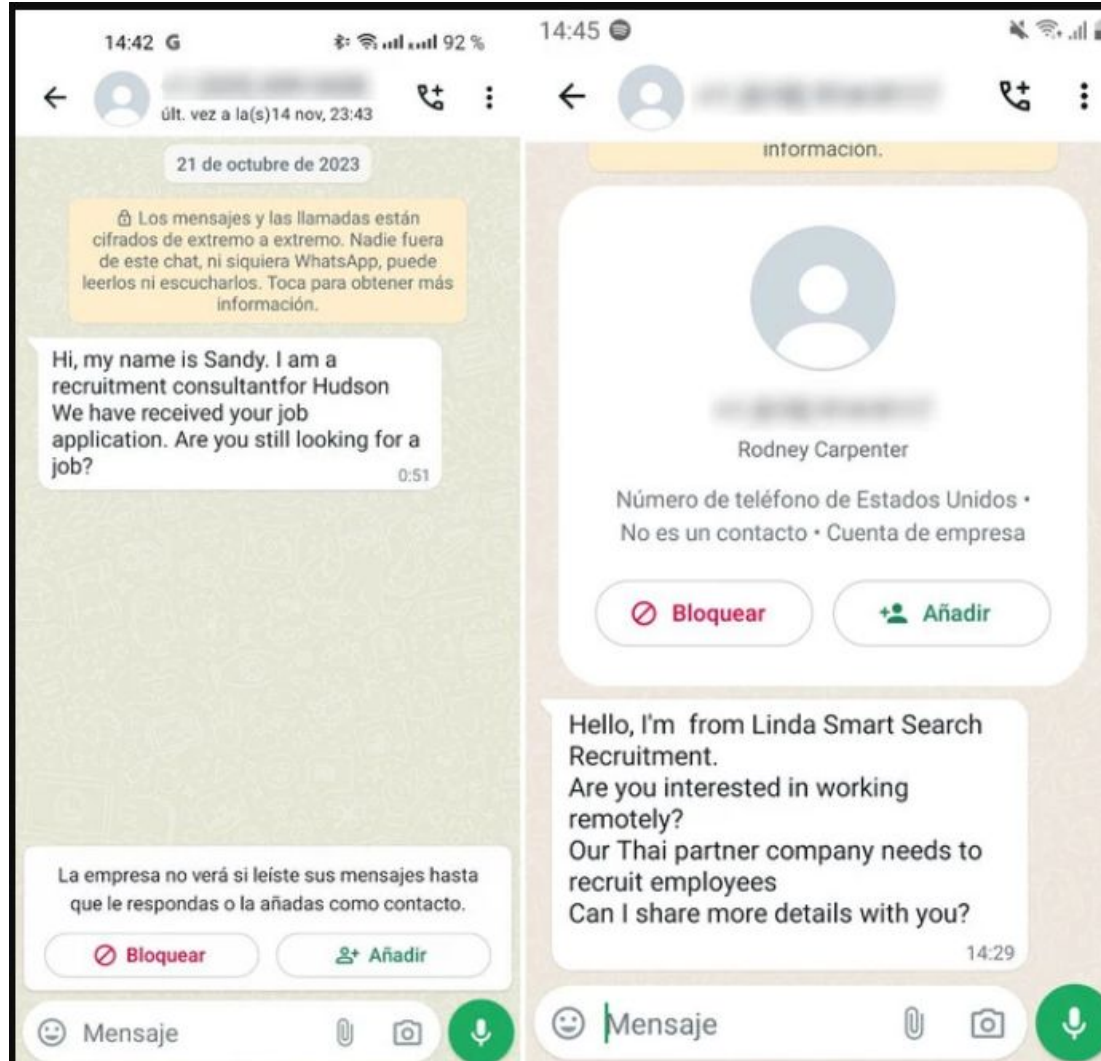
FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

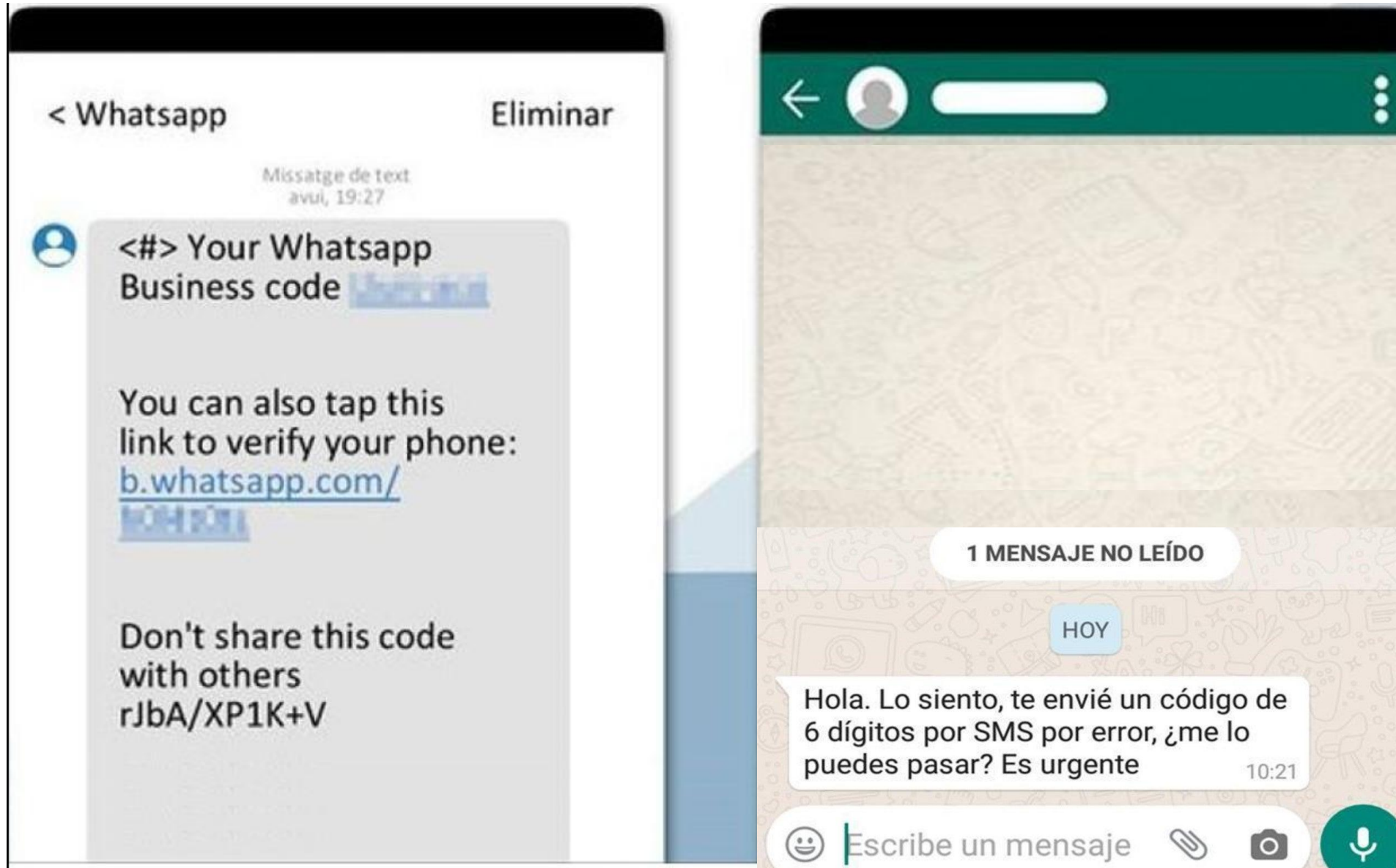
FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

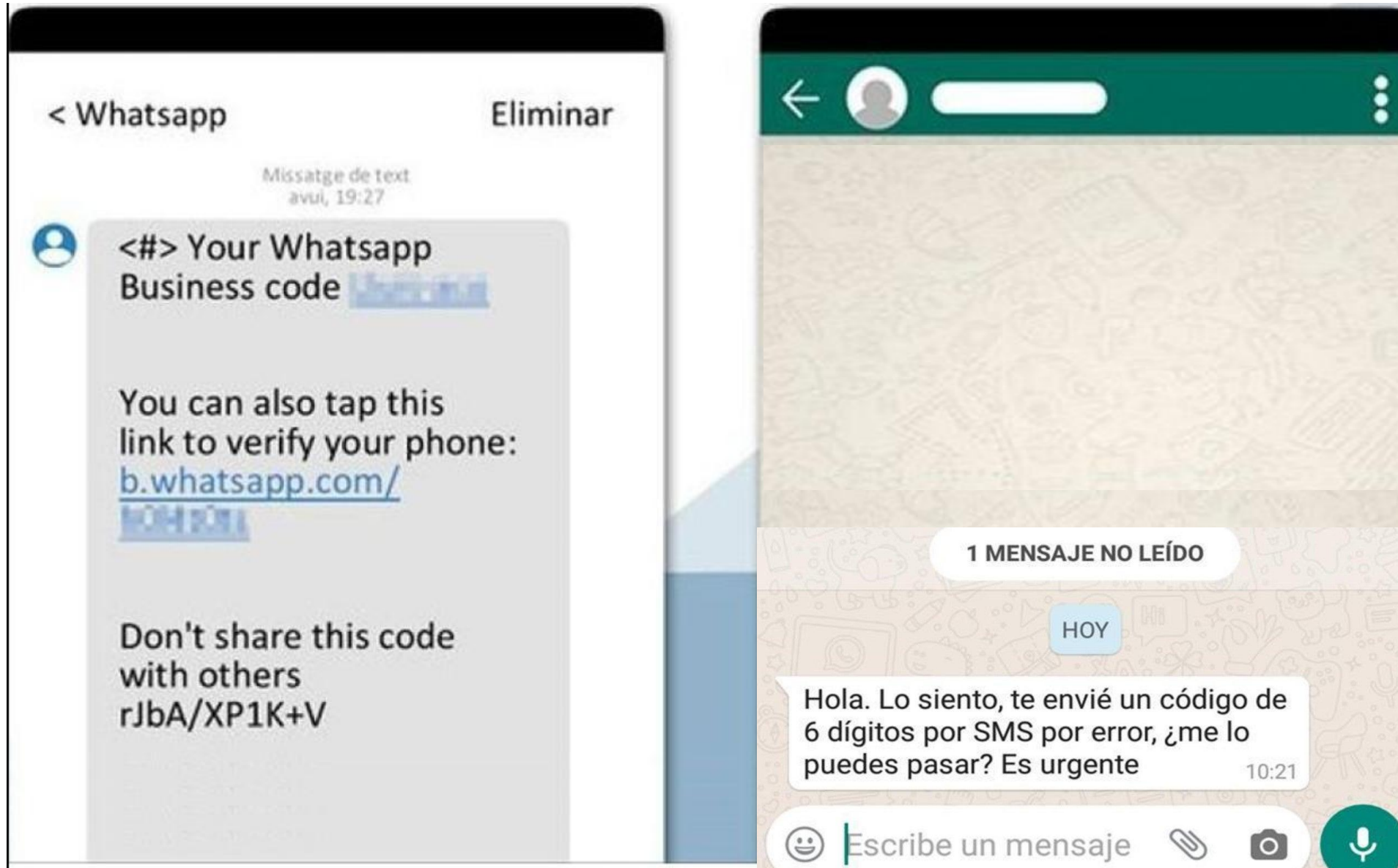
FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Solo WhatsApp puede enviar mensajes.

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Solo WhatsApp puede enviar mensajes.

OTROS CASOS - INCIBE

Caso 1: “Problema en Red Social”

La madre Cibernauta está con su portátil leyendo sus correos. Entre ellos, encuentra uno que le dice que **su cuenta de “Socialnet” está bloqueada momentáneamente por un error interno**. Para poder reactivarla necesita entrar en el enlace que viene en el correo para así poder restablecerla.

Elige la opción que creas correcta para ayudar a la madre Cibernauta

¿Mi red social favorita está bloqueada?
Quizás hayan intentado hackeármela, mejor hacer caso al correo.

¡Es una trampa! Demasiado sospechoso...
¿quién querría robarme la cuenta?



OTROS CASOS - INCIBE

Si es Ingeniería Social

Nos encontramos ante un claro ejemplo de fraude, concretamente de la modalidad ***phishing***.

El ciberdelincuente se hace pasar por una red social para intentar redirigir al usuario a un sitio web fraudulento con el objetivo de robar sus credenciales.

Consejos

- ◆ 1. Accede a la página web o app original de tu red social como haces habitualmente, evitando clicar en el enlace sospechoso.
- ◆ 2. Evita compartir el mensaje con otros usuarios. Así es como se propaga el malware.
- ◆ 3. Contacta con tu red social para reportarles el mensaje sospechoso. Es fácil que descubras que todo funciona bien, y que el mensaje que has recibido solo trataba de engañarte.

ENLACES RELACIONADOS

Conoce a fondo qué es el *phishing*

Ejemplos reales de fraudes de tipo *phishing*



OTROS CASOS - INCIBE

Caso 2: "Factura disponible"

El padre Cibernauta ha recibido un correo con el título "**Tu factura se encuentra disponible**". En él aparece la reciente compra de una aplicación junto con el precio, el método de pago y los últimos dígitos de la tarjeta de crédito. Al final del correo aparece el logo de la empresa acompañado de un enlace a la sección de soporte.

¿Qué crees que debería hacer el padre de la familia Cibernauta?

Probablemente sea cierto, ¿quién lleva la cuenta de las aplicaciones que se descarga?

No me flo... mejor revisar las aplicaciones en mi móvil directamente.



OTROS CASOS - INCIBE

No es Ingeniería Social

Este correo es **legítimo**, está confirmando una compra reciente, realizada por nosotros mismos.

Aparecen datos que únicamente nosotros y la empresa conoce como los detalles del método de pago utilizado.

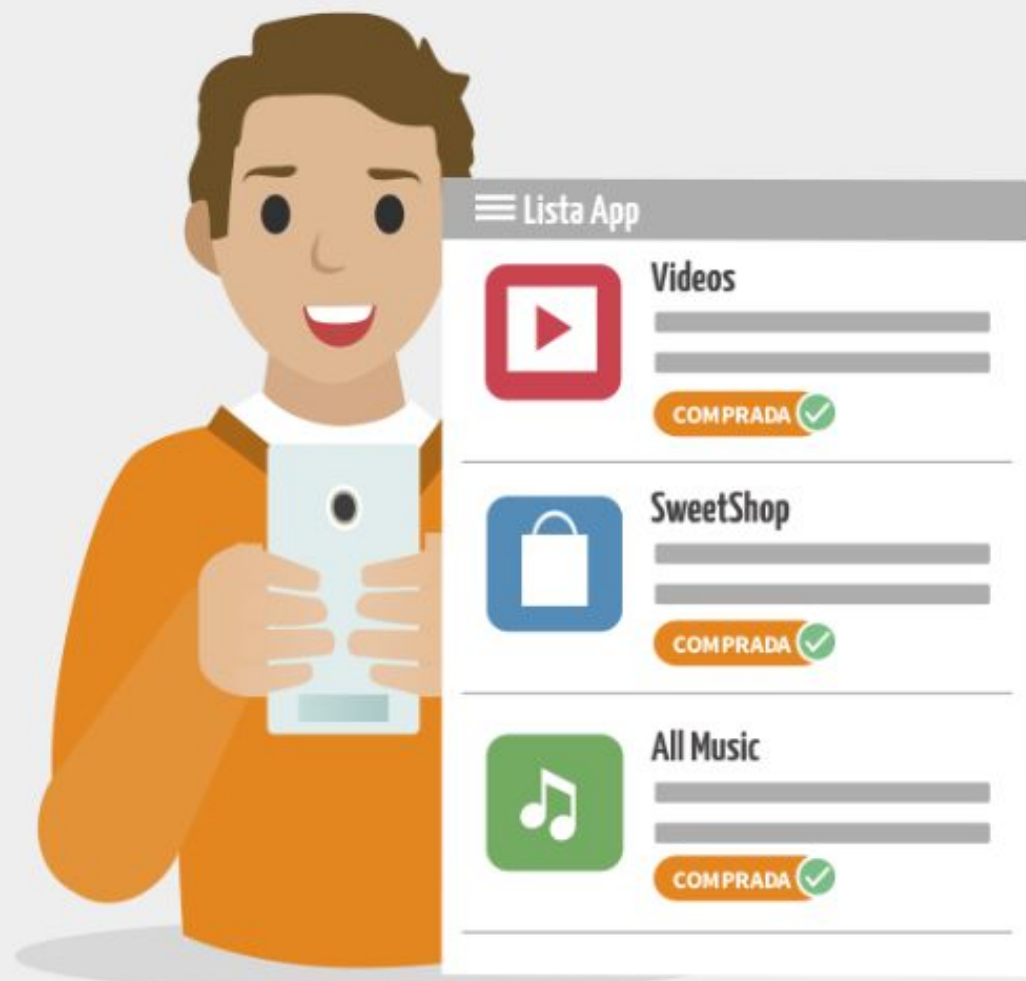
Consejos

- ◆ 1. Lo importante es aplicar el sentido común. Si has realizado una compra recientemente, es posible que la notificación sea legítima, en caso contrario, no.
- ◆ 2. Visita la sección de "tarjetas bancarias" o "movimientos" de tu banca online para revisar que las retenciones correspondan con el importe del producto/servicio adquirido y que no ha habido ningún error por parte del comercio..
- ◆ 3. Ante la menor duda, ponte en contacto con la empresa para verificar toda la información.

Enlaces Relacionados

Compras seguras online

Pagos online seguros (normativa PSD2)



OTROS CASOS - INCIBE

Caso 3: Soporte técnico"

El hijo de la familia recibe una llamada en el móvil de origen desconocido. Al descolgar, **un hombre le dice que está llamando de parte de "Winsoft"**, concretamente, del Departamento de Seguridad asegurando que su ordenador está infectado y que para poder desinfectarlo, debe seguir sus pasos.

¿Cómo ayudarías al hijo Cibernauta?

¡El soporte de este servicio es el mejor!

Para eso ya está mi antivirus, no necesito el soporte de nadie.



OTROS CASOS - INCIBE

Si es Ingeniería Social

Estamos ante un caso de *vishing*.

Por medio de una llamada telefónica intentan engañarnos para que realicemos una serie de acciones con el fin de robar información personal sensible, como por ejemplo, datos personales y bancarios.

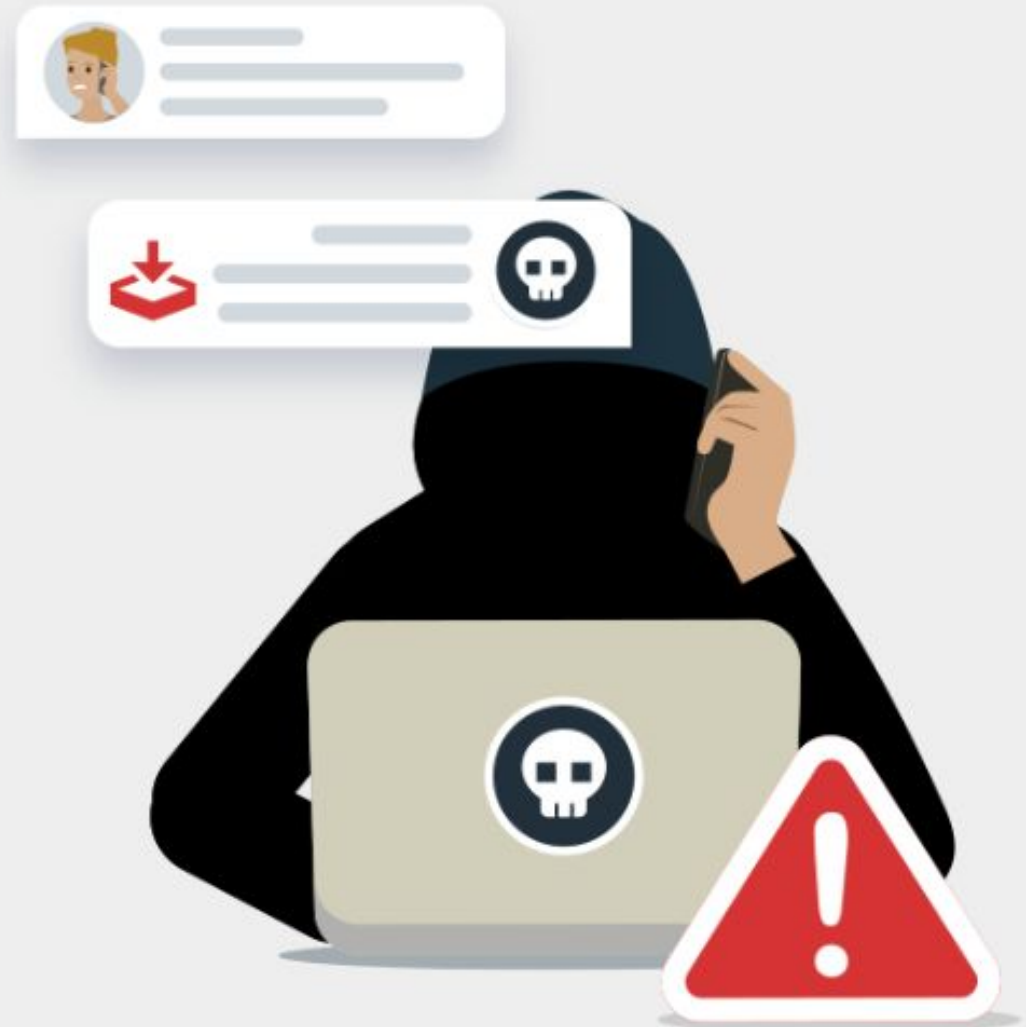
Consejos

- ◆ 1. Ante la mínima duda, cuelga el teléfono.
- ◆ 2. Guárdate el número, te servirá para reconocerlo si vuelven a llamarte de nuevo.
- ◆ 3. Busca el número por Internet, es posible que esté identificado como fraudulento y obtengas más información.

Enlaces Relacionados

¿Microsoft te ha llamado sin haberlo solicitado?

Falso soporte técnico



OTROS CASOS - INCIBE

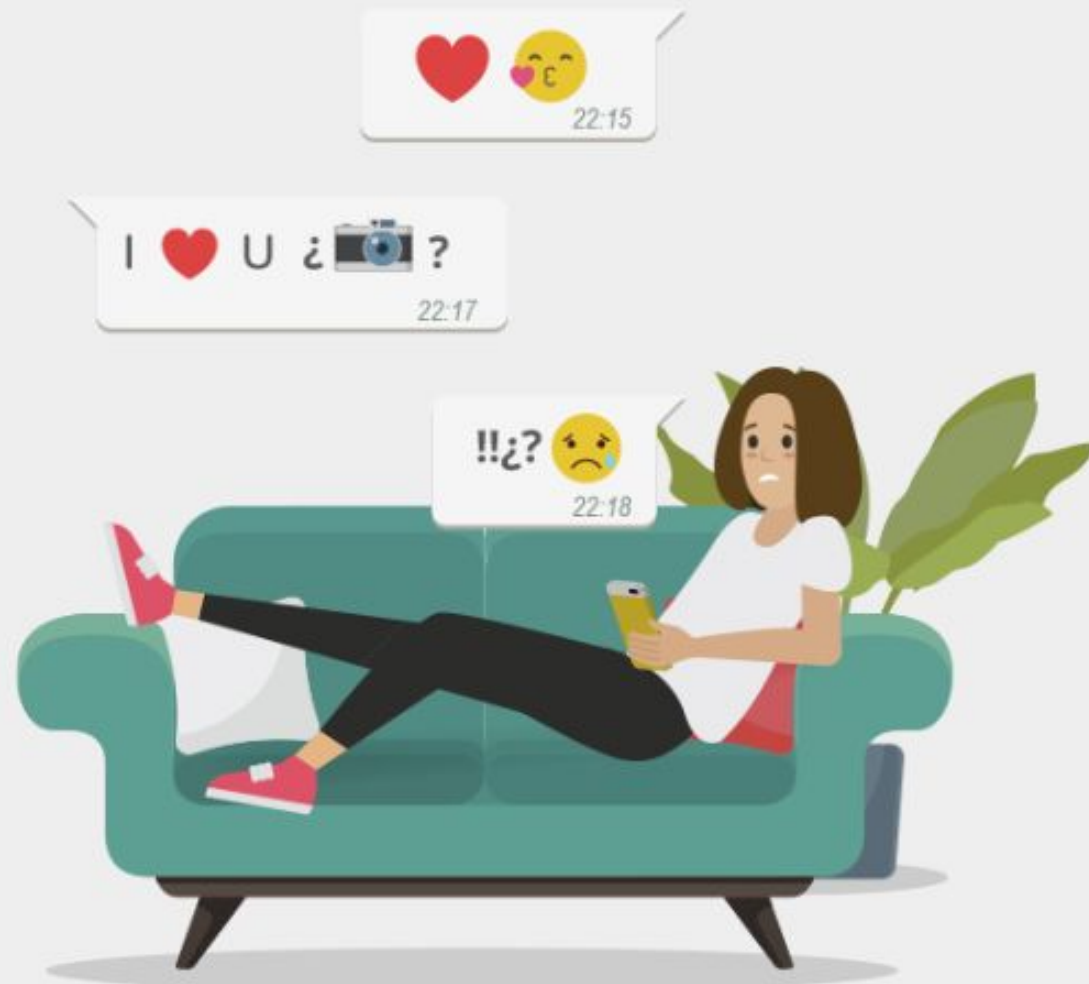
Caso 4: "Relación de pareja"

La hija Cibernauta se encuentra **chateando con un chico con el que lleva hablando meses**. Parece que la relación es cada vez más íntima y en esta ocasión incluso subida de tono. En un momento, el chico le pide algunas fotos sin ropa.

¿Qué debería hacer la hija Cibernauta?

Nunca envíes fotografías o vídeos comprometedores. Pueden volverse en tu contra.

No es un desconocido ni una amenaza si llevan tanto tiempo hablando e intercambiando correos.



OTROS CASOS - INCIBE

Si es Ingeniería Social

Estamos ante un caso de *sexting*.

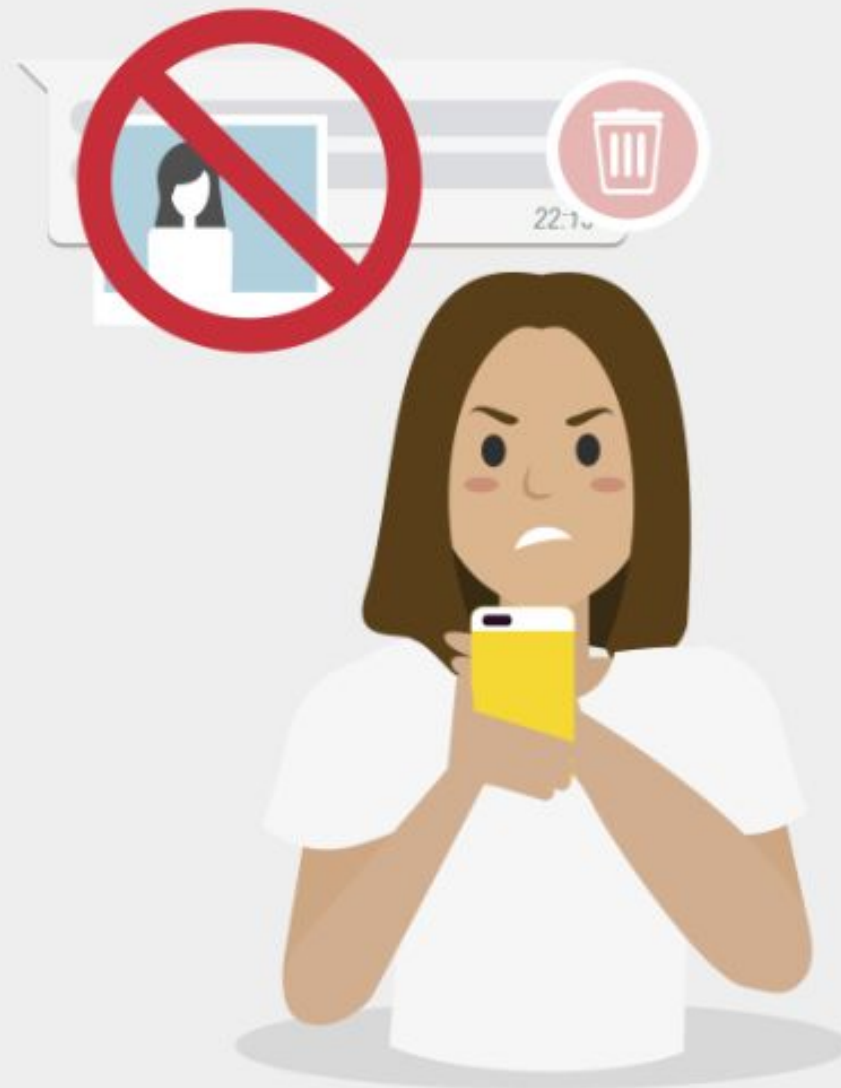
Este tipo de actividades nunca acaban bien. No importa la relación que tengas, no sabes donde podrá acabar este material ni el uso que va a hacer esta persona del mismo. Podría ser usado para chantajearnos a cambio de dinero o material cada vez más comprometedor.

Consejos

- ◆ 1. Sé consciente de todo lo que compartes por Internet, piensa que podría hacerse público y acabar en manos de un ciberdelincuente que lo utilice para extorsionarte.
- ◆ 2. Si te extorsionan por Internet para que realices un pago económico a cambio de no difundir material comprometido, no accedas a las peticiones, no evitará que difundan los contenidos ni que continúen los chantajes.
- ◆ 3. Si tienes material que no quieres que acabe en malas manos, asegúrate de cifrarlo, utilizando contraseñas robustas.

➤ Enlaces Relacionados

Correos electrónicos simulando sextorsión.



OTROS CASOS - INCIBE

Caso 5: "Problema en usb"

El hijo Cibernauta está en la cafetería de la universidad. **En la mesa donde está sentado, hay un dispositivo USB.** Pregunta a su alrededor si es de alguien pero nadie sabe de quién es. Decide conectarlo al portátil para ver si tiene algún archivo reconocible y así poder entregárselo a su dueño. Según lo conecta, el portátil se apaga inesperadamente, pero inmediatamente se vuelve a encender sin problemas.

¿Qué debería hacer el hijo Cibernauta ahora?

Trato de conectarlo de nuevo y si da problemas, lo intento desde otro dispositivo.

¡Cuidado! No sabemos de quién es, ni qué ficheros contiene.



OTROS CASOS - INCIBE

Si es Ingeniería Social

Podríamos estar ante un caso de ingeniería social conocido como ***baiting***.

Se abandonan dispositivos USB con la intención de que alguien los encuentre y los conecte a sus dispositivos descargando y ejecutando *malware* en ellos.

Consejos

- ◆ 1. Usa programas de detección y limpieza como son los programas antivirus para prevenir infecciones.
- ◆ 2. Si no estás seguro de que tu dispositivo esté libre de *malware*, sigue los pasos que encontrarás en **Desinfecta tus dispositivos**.
- ◆ 3. Comprueba periódicamente que tanto el antivirus, como el sistema operativo y demás programas, están actualizados a su última versión para mayor seguridad.

Enlaces Relacionados

[Puesta a punto de tus dispositivos](#)

[Herramientas gratuitas de seguridad](#)

[Servicio AntiBotnet](#)



OTROS CASOS - INCIBE

Caso 6: "Cupón WhatsApp"

Una amiga de la madre Cibernauta le **envió un enlace por WhatsApp con un cupón de 100€ para gastar en unos conocidos grandes almacenes**. Rápidamente hizo clic en el enlace y siguió todos los pasos indicados para conseguirlo: cumplimentó una encuesta, compartió la promoción con sus contactos y facilitó sus datos personales.

¿Crees que la madre hizo lo correcto? Marca la opción que creas correcta

¡Qué bien! Hay que aprovecharlo

¿Para qué querrán tanta información sobre mí?



OTROS CASOS - INCIBE

Si es Ingeniería Social

Fraude de tipo *phishing* muy común que se propaga por WhatsApp para llegar a más usuarios.

Bajo la apariencia de ser un mensaje que regala un cupón o vale de descuento en empresas conocidas, nos engañan para robar nuestros datos privados e incluso bancarios.

Consejos

- ◆ 1. Precaución al seguir enlaces en correos, en SMS, mensajes en WhatsApp o en redes sociales aunque sean de contactos conocidos.
- ◆ 2. Sé cauto con los mensajes que dicen regalarte cosas a cambio de nada, contrasta la información y en caso de duda no accedas a sus peticiones.
- ◆ 3. Si has facilitado información personal, vigila regularmente qué información tuya circula por Internet. Una simple búsqueda en Google puede decirte muchas cosas.

🔍 Enlaces Relacionados

Cómo configurar y usar WhatsApp de forma segura



OTROS CASOS - INCIBE

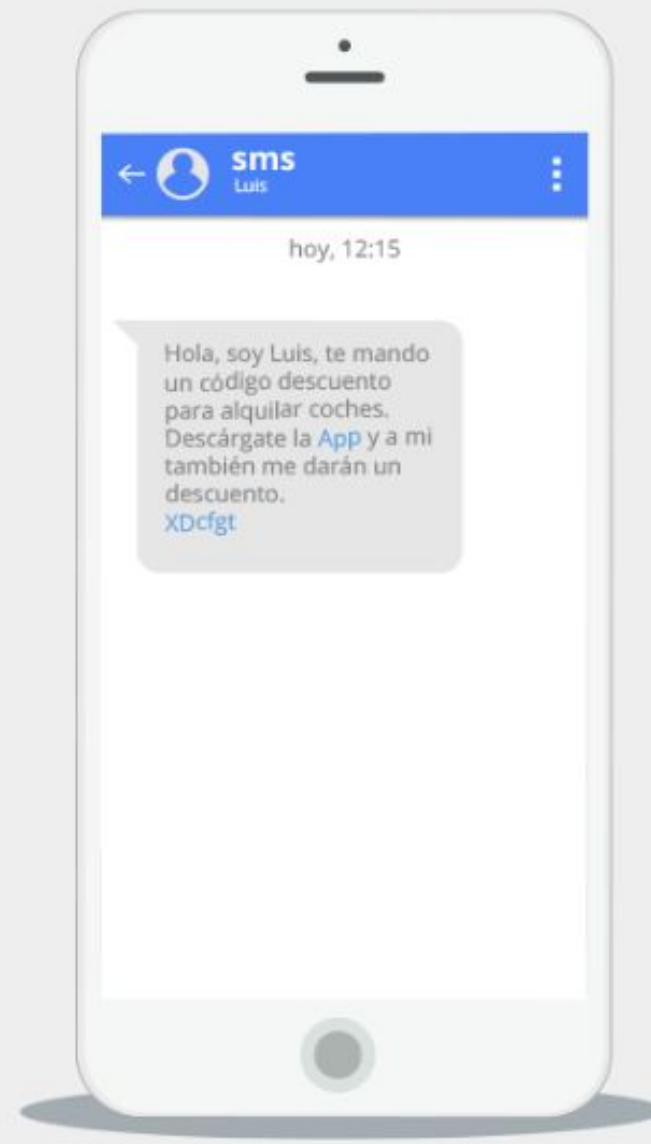
Caso 7: "Código SMS"

Un amigo del padre Cibernauta le ha enviado un **mensaje de texto para que utilice un código de descuento**. De esta forma, él también recibiría un descuento en la misma aplicación para alquilar coches. El padre rápidamente abre la aplicación y pega el código a la espera de que en su próximo alquiler tenga un descuento.

Elige tu opción, ¿hubieras hecho lo mismo que el padre Cibernauta?

**¡No podemos desaprovechar esta oportunidad!
Además, no hay de qué preocuparse, es solo una
promoción con descuentos.**

**¡Mucho ojo! Las ofertas online hay que mirarlas con
lupa.**



OTROS CASOS - INCIBE

No es Ingeniería Social

Este SMS es legítimo.

Es una práctica comercial puesta en marcha por empresas para la captar nuevos clientes. No obstante, hay que prestar atención a las recomendaciones.

Consejos

- ◆ 1. Habla con quien te lo ha enviado para asegurarte de que es un mensaje legítimo y vigila la letra pequeña de la oferta.
- ◆ 2. Revisa qué datos estás cediendo y a quién a cambio de beneficiarte del descuento. Es posible que tus datos vayan a ser cedidos a terceras empresas con fines comerciales.
- ◆ 3. Pese a que este caso pueda ser legítimo, también puede ser que el mensaje que ha recibido el padre Cibernauta no haya sido enviado realmente por su amigo. Es ese caso estaríamos hablando de un intento de estafa enviado en nombre de alguien, suplantando su identidad.

Enlaces Relacionados

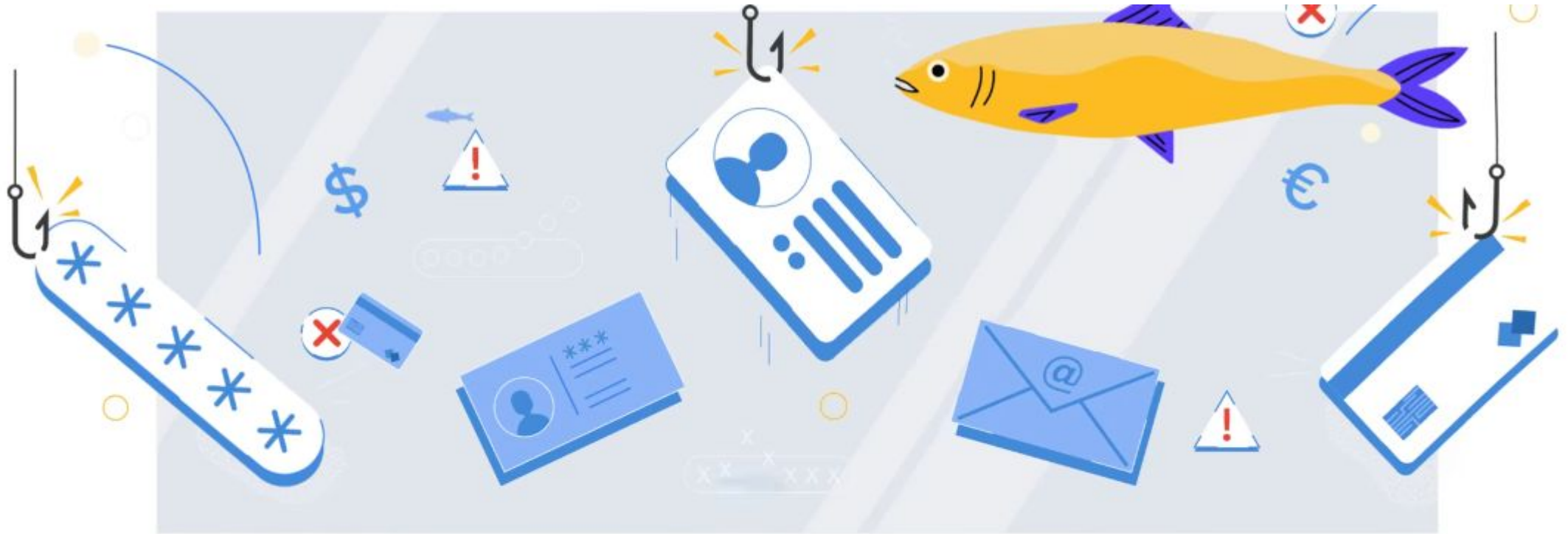
Cuando el producto somos nosotros.

Evita el spam con unas sencillas pautas.



TEST

<https://phishingquiz.withgoogle.com/?hl=es>



¿Puedes detectar cuándo te están
engañando?

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Luís Gómez <luis.gomez8000@gmail.com>
para mí ▾

Luís Gómez ha compartido un enlace al siguiente documento:

 [Presupuesto de departamento del 2024.docx](#)



Hola. Aquí tienes el documento que querías. Dime si necesitas algo más.

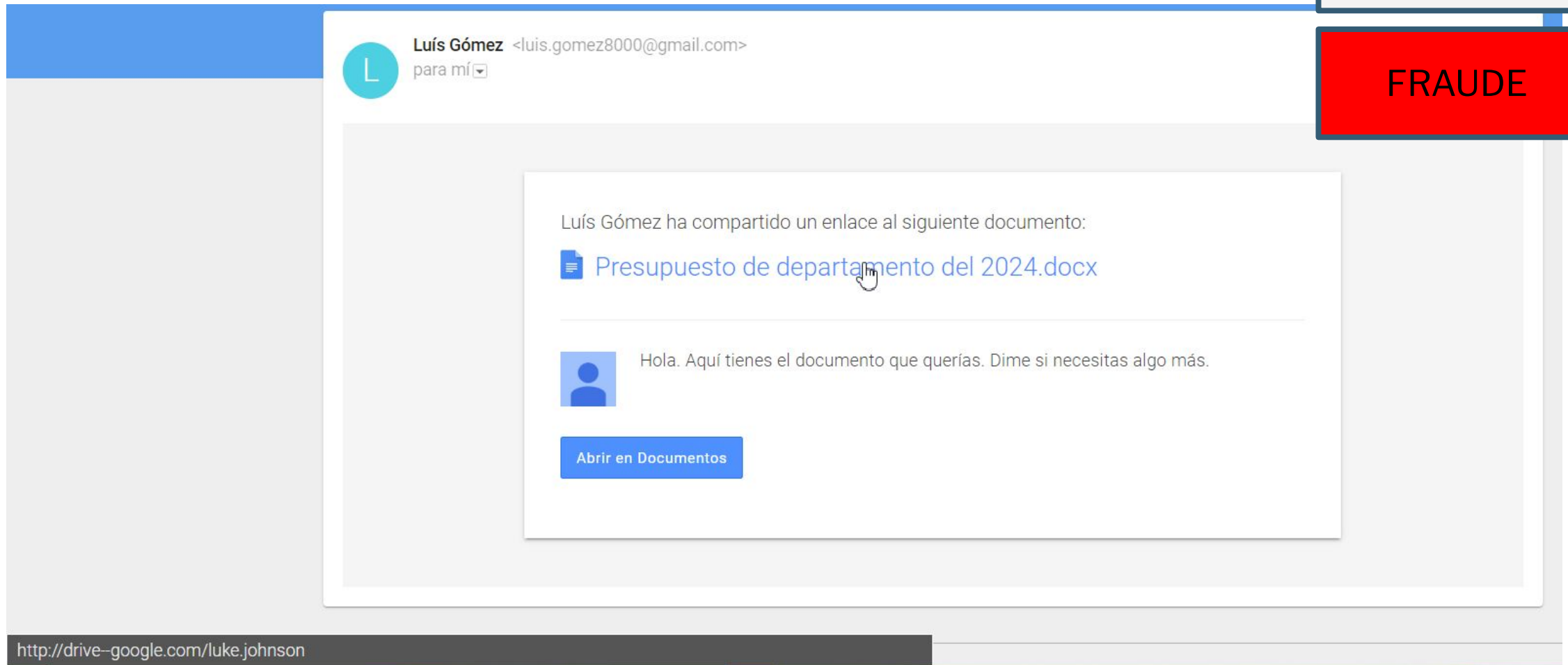
Abrir en Documentos

<http://drive-google.com/luke.johnson>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



http://drive-google.com/luke.johnson

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Mensaje de fax - No responder [administrador] <noreply@efacks.com>
para mí ▾

Recibiste un fax de 1 página el 2/2/24, 17:50

[Ver este fax online](#)



Gracias por utilizar el servicio de eFax. Si tienes alguna pregunta o crees que has recibido este fax por error, visita: www.efax.es/preguntas-mas-frecuentes.

eFax Inc (c) 2024

... JTGSAW | Google
<http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Mensaje de fax - No responder [administrador] <noreply@efacks.com>

para mí ▾

17:50

La dirección del remitente es "efacks.com" (está mal escrita). En la siguiente pregunta, prueba a analizar el encabezado para ver más detalles.

Siguiente

info@elcorreoelectronico.com

Nombre del usuario

Organización

Tipo

Dominio



Gracias por utilizar el servicio de eFax. Si tienes alguna pregunta o crees que has recibido este fax por error, visita: www.efax.es/preguntas-mas-frecuentes.

eFax Inc (c) 2024

http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



José <jose867530@gmail.com>
para mí ▾

17:52

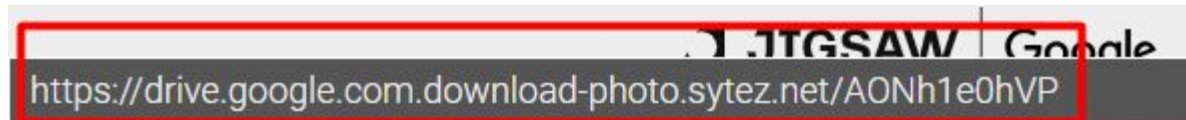
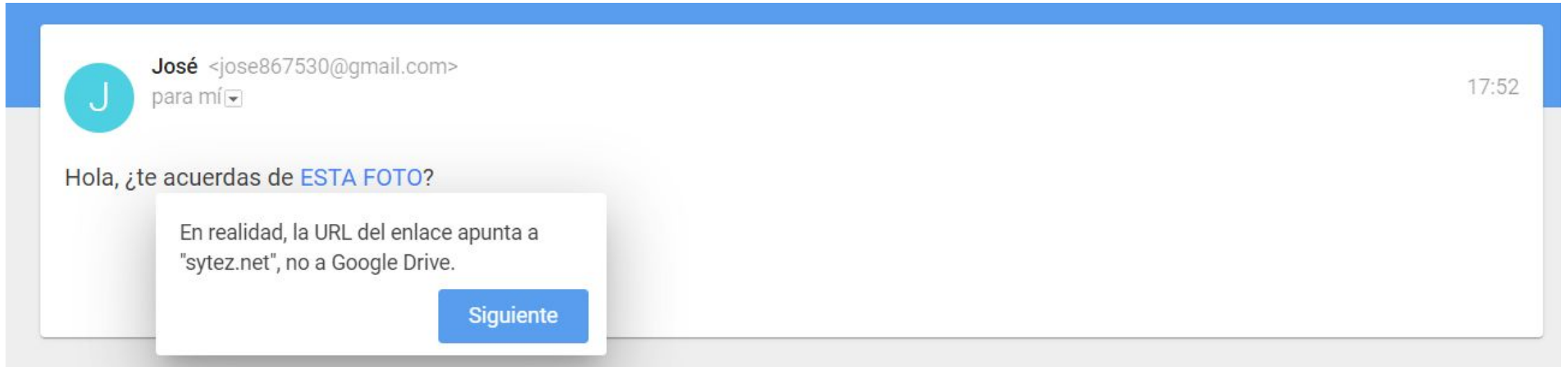
Hola, ¿te acuerdas de [ESTA FOTO?](#)

<https://drive.google.com/download-photo.sytez.net/AONh1e0hVP>

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Dropbox <no-reply@dropboxmail.com>
para mí

17:53



Hola:

Tu Dropbox está lleno y ha dejado de sincronizar archivos. No podrás acceder a los nuevos archivos que añadas a tu carpeta de Dropbox desde el resto de tus dispositivos. Tampoco se creará una copia de ellos online.

Actualiza tu versión de Dropbox hoy mismo y consigue 1 TB (1000 GB) de espacio, así como eficientes funciones para compartir contenido.

Actualiza tu Dropbox

Para ver otras formas de conseguir más espacio, visita nuestra página [Obtener más espacio](#).

¡Que disfrutes de Dropbox!

El equipo de Dropbox

P. D.: Si necesitas el plan más grande del que disponemos, echa un vistazo a [Dropbox Business](#).

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

**Dropbox** <no-reply@dropboxmail.com>
para mí ▾ 17:53

Si buscas "dropboxmail.com", verás rápidamente que es legítimo.

Siguiente



Tu Dropbox está lleno y ha dejado de sincronizar archivos. No podrás acceder a los nuevos archivos que añadas a tu carpeta de Dropbox desde el resto de tus dispositivos. Tampoco se creará una copia de ellos online.

Actualiza tu versión de Dropbox hoy mismo y consigue 1 TB (1000 GB) de espacio, así como eficientes funciones para compartir contenido

Actualiza tu Dropbox

Para ver otras formas de unirte a Dropbox, visita [dropbox.com](#)

¡Que disfrutes de Dropbox

El equipo de Dropbox

P. D.: Si necesitas el plan más grande del que disponemos, echa un vistazo a [Dropbox Business](#).

La URL es un enlace legítimo y seguro a "dropbox.com".

Siguiente

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Por lo general, sus correos electrónicos proceden de "sara.martin@centrowestmount.org".



Sara Martín <sara.martin@escuelawestmount.org>
para mí ▾

17:54

Buenos días, Belen:

Adjunto el informe de actividad financiera del 2024 para que lo revise.

Gracias y un saludo,

Sara Martín
Colegio Montellano

PDF

PDF

I.A.F. del 2024.pdf

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE

Por lo general, sus correos electrónicos proceden de "sara.martin@centrowestmount.org".



Sara Martín <sara.martin@escuelawestmount.org>

para mí ▾

17:54

La dirección del remitente es ligeramente diferente a la que has visto anteriormente: "sara.martin@centrowestmount.org".

Siguiente

Colegio Montellano

PDF

PDF

I.A.F. del 2024.pdf

PDF

PDF

I.A.F. del 2024.pdf

Ten cuidado al abrir archivos PDF, sobre todo si no los esperas.

Siguiente

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Google <no-reply@google.support>
para mí ▾

17:56

Alguien tiene tu contraseña

Hola:

Alguien acaba de utilizar tu contraseña para intentar iniciar sesión en tu cuenta de Google.

Información:

viernes, 2 de febrero de 2024, 17:56:14 (GMT+01:00)

Slatina, Rumanía

Navegador Firefox

Google ha detenido este intento de inicio de sesión. Debes cambiar tu contraseña de inmediato.

[CAMBIAR CONTRASEÑA](#)

Un saludo,

El equipo de Mail

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Google <no-reply@google.support>
para mí

17:56

La dirección de remitente "google.support"
no se utiliza.

Siguiente

Información:

viernes, 2 de febrero de 2024, 17:56:14 (GMT+01:00)
Slatina, Rumanía
Navegador Firefox

Google ha detenido este intento de inicio de sesión. Debes cambiar tu contraseña de inmediato.

CAMBIAR CONTRASEÑA

Un saludo,

El equipo de Mail

CAMBIAR CONTRASEÑA

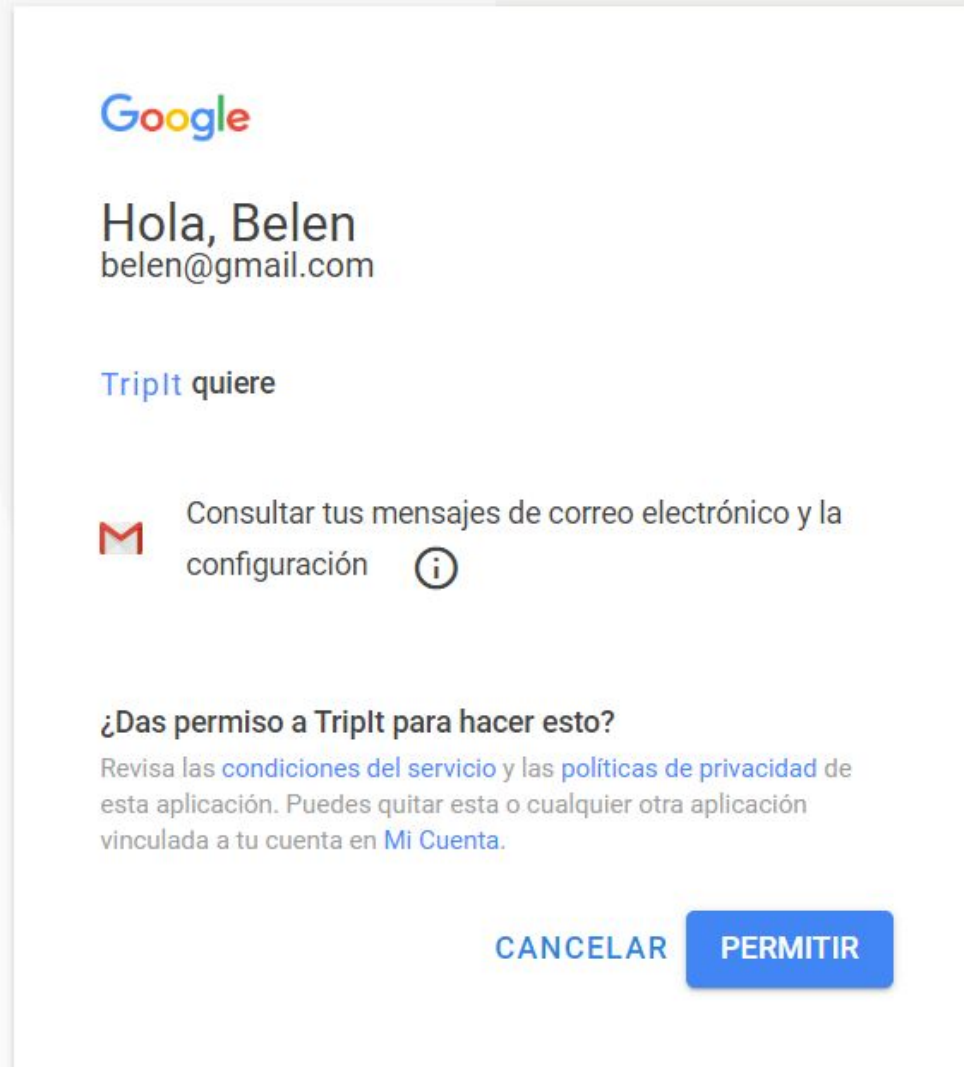
Este enlace apunta a un subdominio de
"ml-security.org", no de Google.

Siguiente

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Te has registrado en un servicio de planificación de viajes. Quieres iniciar sesión con tu correo, pero fíjate detenidamente.

JUEGO: ¿VERDAD O FRAUDE?

VERDAD

FRAUDE



Hola, Belen
belen@gmail.com

Triplt quiere

Aquí se muestra el nombre de la aplicación que solicita permiso, aunque debes hacer clic en ella para asegurarte de que el resto de los datos sean correctos.

Siguiente

Revisa las [condiciones del servicio](#) y las [políticas de privacidad](#) de esta aplicación. Puedes quitar esta o cualquier otra aplicación vinculada a tu cuenta en [Mi Cuenta](#).

CANCELAR

PERMITIR

Te has registrado en un servicio de planificación de viajes. Quieres que analicen tu correo, pero fíjate detenidamente.

VIDEO: El negocio de los datos robados

<https://www.rtve.es/play/videos/la-hora-de-la-1/negocio-compra-datos-personales-internet/6937155/>

Verificación en dos pasos

Activar la verificación en dos pasos

Con la verificación en dos pasos, también denominada "autenticación de dos factores", puedes añadir una capa adicional de seguridad a tu cuenta por si te roban la contraseña. Después de configurar la verificación en dos pasos, puedes iniciar sesión en tu cuenta con lo siguiente:

- Tu contraseña
- Tu teléfono

<https://support.google.com/accounts/answer/185839?hl=es-4199>

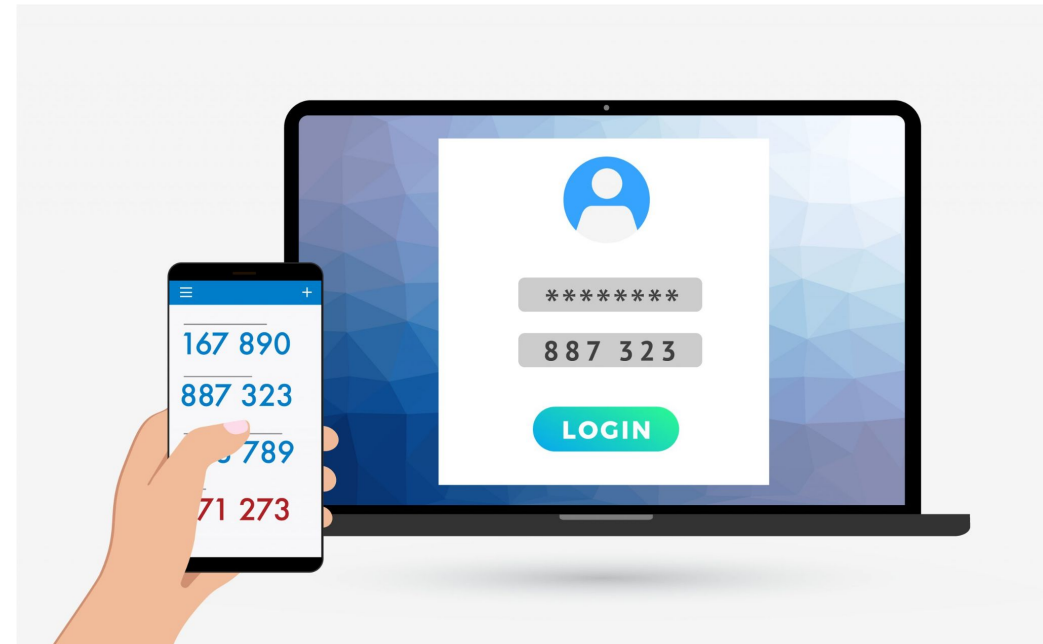
Verificación en dos pasos

Activar la verificación en dos pasos

Con la verificación en dos pasos, también denominada "autenticación de dos factores", puedes añadir una capa adicional de seguridad a tu cuenta por si te roban la contraseña. Después de configurar la verificación en dos pasos, puedes iniciar sesión en tu cuenta con lo siguiente:

- Tu contraseña
- Tu teléfono

[Activar Verificación en 2 pasos en Google](#)



Verificación en dos pasos: Google

[Activar Verificación en 2 pasos en Google](#)

Iniciar sesión en Google



Contraseña

Última modificación: 9 ene 2020

>

Verificación en dos pasos

 Activado

>

Contraseñas de aplicaciones

Ninguna

>

Métodos para verificar tu identidad

Podemos usar estas opciones en caso de que tengamos que comprobar tu identidad cuando inicies sesión o para contactar contigo si detectamos actividad sospechosa en tu cuenta



Teléfono de recuperación

649 86 64 90

>

Correo electrónico de recuperación

Poriphone@gmail.com

>

← Verificación en dos pasos

**Aplicación Authenticator**
Authenticator en Android
Fecha en que se ha añadido: 9 de diciembre de 2019
[CAMBIAR TELÉFONO](#)

**Mensaje de voz o de texto**
649 86 64 90 **Verificado**
Los códigos de verificación se envían a través de mensajes de texto.
[AÑADIR TELÉFONO](#)

Añadir más segundos pasos para verificar la identidad

Configura pasos de seguridad adicionales para iniciar sesión cuando tus otras opciones no estén disponibles.

**Códigos de seguridad**
Estos códigos imprimibles de un solo uso te permiten iniciar sesión cuando no tengas tu teléfono cerca, como cuando estás de viaje.
[CONFIGURAR](#)

**Llave de seguridad**
La llave de seguridad es un método de verificación que te permite iniciar sesión de forma segura. Estas llaves pueden estar integradas en tu teléfono, utilizar Bluetooth o conectarse directamente al puerto USB de tu ordenador.
[AÑADIR LLAVE DE SEGURIDAD](#)

Verificación en dos pasos: Google

Activar Verificación en 2 pasos en Google



Google

Verificación en dos pasos

Este paso extra nos indica que eres tú quien está intentando iniciar sesión



Consulta tu dispositivo

Google ha enviado una notificación a tu Samsung Galaxy S10+, a tu Samsung Galaxy S10+ y a 1 dispositivos más. Toca **Sí** en la notificación para continuar.

También puedes abrir la aplicación Gmail en tu iPad, en tu iPhone 7 Plus o en tus otros 1 dispositivos para iniciar sesión desde ellos.

☒ No volver a preguntar en este ordenador

[Probar de otra manera](#)

Español (España) Ayuda Privacidad Términos

Google

¿Estás intentando iniciar sesión?

Dispositivo
CPU OS 12_4 like Mac OS X

Cerca de
España

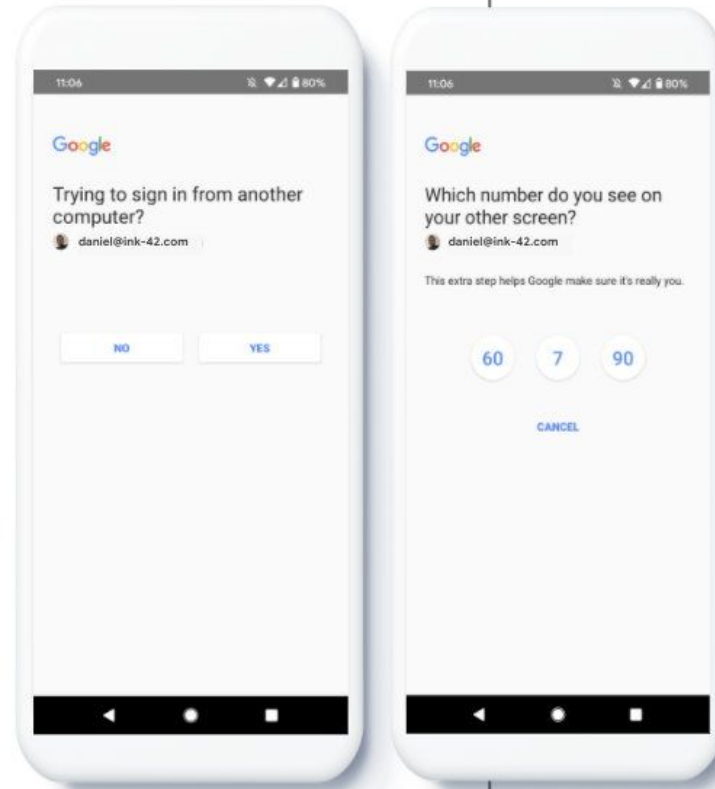
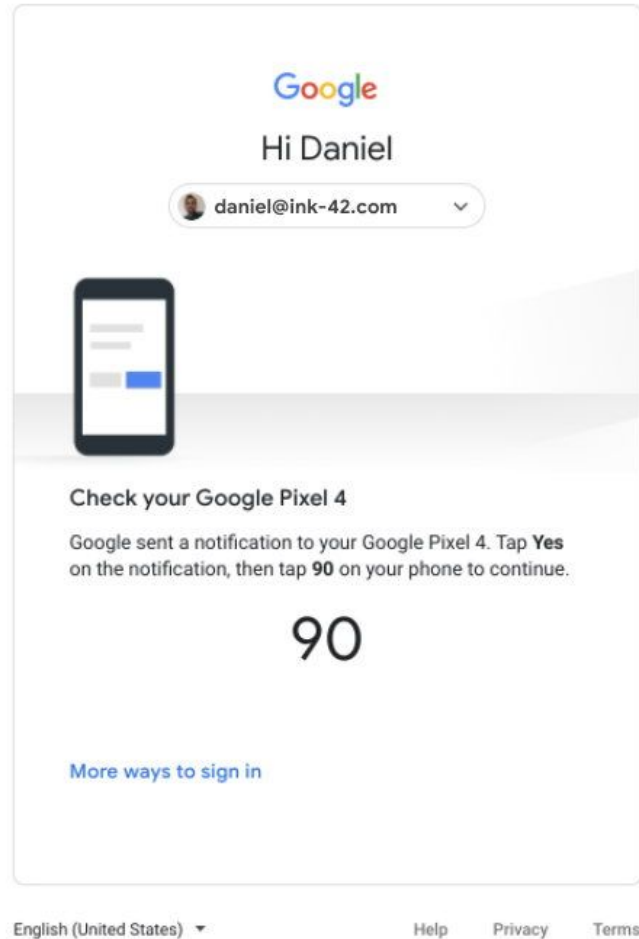
Hora
Ahora mismo

[NO, NO SOY YO](#) [sí](#)

Sesión iniciada

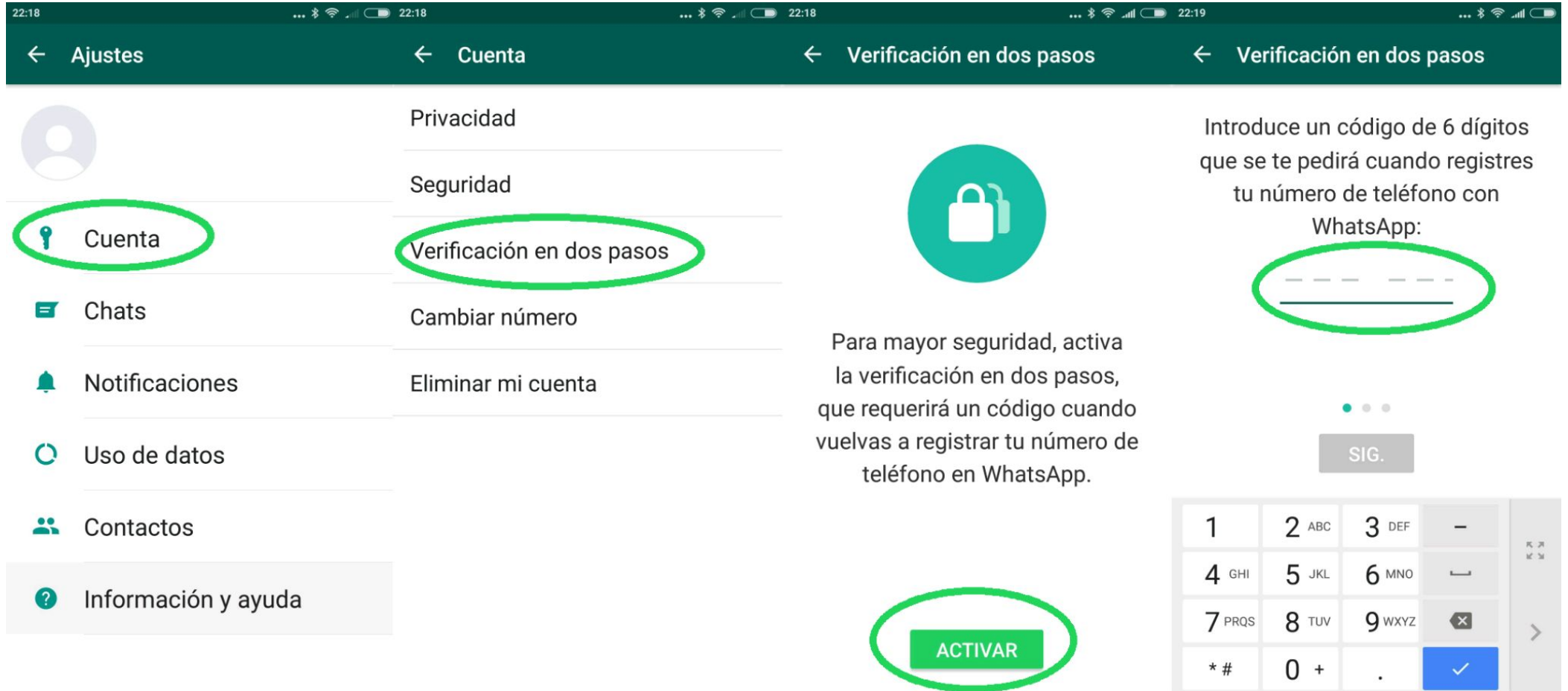
Verificación en dos pasos: Google

Activar Verificación en 2 pasos en Google



Verificación en dos pasos: WhatsApp

Activar Verificación en 2 pasos en WhatsApp



Verificación en dos pasos: WhatsApp

Activar Verificación en 2 pasos en WhatsApp

← Verificación en dos pasos

Verificación en dos pasos

← Verificación en dos pasos

Confirma tu dirección de correo electrónico:

Correo

GUARDAR

1 2 3 4 5 6 7 8 9 0

q w e r t y u i o p

@ # \$ % & * ' () ñ

a s d f g h j k l

↑ z x c v b n m

?123 @ . ✓

La verificación en dos pasos está activa.

OK

La verificación en dos pasos está activa. Necesitarás introducir tu código cuando vuelvas a registrar tu número de teléfono en WhatsApp.

✕

Desactivar

Cambiar código

✓

Cambiar dirección de correo

RECOMENDACIONES para protegernos

01 | Phishing

Aprendiendo a identificar fraudes online Pag. 03/12



“Recibí un email, supuestamente de mi tienda online favorita, que detallaba que estaban regalando varios productos por tiempo limitado. Solo tenía que entrar en el enlace y completar varios campos.

Me interesó, así que los rellené, incluyendo mi nombre, dirección y datos de mi tarjeta de crédito. Días más tarde me di cuenta de que faltaban 600€ en mi cuenta.”



¿Cómo nos afectaría?

Suplantando la identidad de personas, entidades y servicios conocidos, el ciberdelincuente es capaz de engañarnos para que le facilitemos información personal. Para ello, crean correos electrónicos y mensajes que utilizan como redamo para que finalmente accedamos a una web fraudulenta.



Comprobar la ortografía y redacción

Muchos de los correos de phishing contienen errores ortográficos y de redacción, no son propios de entidades debido al uso de traductores automatizados.



Verificar que la cuenta es original

Debemos comprobar que el email coincide con la empresa que nos envía el correo. Generalmente utilizan dominios públicos o que se parecen al que sería el correo oficial.

Por ejemplo: [google.com](https://www.google.com) en vez de [google.com](https://www.google.com)

Recomendaciones "Buenas prácticas del cibernauta"



Revisar la URL

Los enlaces del correo deben ser comprobados. Antes de hacer clic, podemos colocar el cursor del ratón sobre el hipertexto para ver la URL a la que nos redirige.



No descargar archivos adjuntos

Bajo ningún concepto descargaremos archivos adjuntos del email si no podemos confirmar que se trata de un mensaje legítimo.

Enlaces relacionados

- Conoce a fondo qué es el phishing
- No hagas clic en todo lo que lees
- Phishing. No muerdas el anzuelo



Oficina
de Seguridad
del Internauta

RECOMENDACIONES para protegernos

03 | Tienda online fraudulentas

Aprendiendo a identificar fraudes online Pag. 05/12



"Me encontraba navegando por Internet, buscando un par de zapatos nuevos que comprar, cuando encontré una oferta estupenda.

Estaban un 40% más baratos que en la tienda oficial, y me decidí a comprarlos. La web parecía fiable, aunque ya han pasado dos meses desde que los pedí y aún no me han llegado."



¿Cómo nos afectaría?

Robo de nuestro dinero e información personal al acceder a las tiendas online a través de anuncios con ofertas irresistibles. Además, lo más habitual es que no recibamos el producto comprado o de recibirlo, que se trate de una falsificación.



Observar el aspecto visual

Una web mal construida y poco atractiva puede ser debido a que se ha hecho con prisas y/o tratando de copiar el estilo de una tienda oficial.



Monitorizar opiniones

Antes de comprar un producto revisaremos las opiniones de otros usuarios haciendo una búsqueda por Internet.

Comprobar información legal empresa

El NIF de la empresa y otros datos como la razón social o los datos de contactos son necesarios para identificar a una tienda online fiable.

Fijarse en los precios

Deben hacernos sospechar los precios demasiado bajos con respecto a las tiendas oficiales o al precio de mercado.

Recomendaciones "Buenas prácticas del cibernauta"



Comprobar certificado SSL

Las tiendas online fiables tendrán una conexión segura por HTTPS y contarán con un certificado de seguridad.

Leer condiciones y políticas

Seamos conscientes de las condiciones del servicio que se nos está ofreciendo, así como de las políticas de privacidad de la plataforma. Esta información suele incluirse dentro del "Aviso legal" de la web, y debemos sospechar si no lo vemos por ningún lado.

Analizar pagos permitidos

Evitaremos páginas que, aunque contengan los logos de muchos métodos de pago online, a la hora de la verdad solo permiten transferencias a depósitos y pagos con tarjeta.

Contrastar reputación en la red

Un rápido vistazo por Internet, buscando por el nombre de la empresa o del vendedor, nos dirá si nos encontramos ante una estafa o fraude.

Enlaces relacionados

- Campaña concienciación sobre "Compras seguras online"
- Guía de "Compra segura en Internet"
- Tiendas online fraudulentas



Oficina
de Seguridad
del Internauta

RECOMENDACIONES para protegernos

04 | Falsos alquileres

Aprendiendo a identificar fraudes online Pág. 06/12



"Mi novia y yo planeábamos alquilar un piso en la playa en verano. Buscando en una app de alquileres vacacionales dimos con un anuncio muy interesante. El precio era mucho mejor que el de otros apartamentos de la zona, así que decidimos alquilarlo. Cuando llegamos al destino nos encontramos con que el supuesto apartamento no era del propietario con el que habíamos contactado. De hecho, ni si quiera estaba en alquiler."



¿Cómo nos afectaría?

Ponen en circulación **anuncios de inmuebles demasiado buenos** como para dejarlos pasar. Una vez mostramos interés, tratarán de obtener nuestro dinero lo antes posible pidiendo, por ejemplo, **pequeños pagos en concepto de fianza o reserva**.



Analizar el perfil vendedor

Revisaremos el perfil del vendedor, leeremos las valoraciones de otros clientes y comprobaremos la antigüedad del perfil o los datos de contacto.



Revisar las descripciones

Descripciones que contengan errores ortográficos o frases inconexas pueden indicar que el anuncio es falso.



Comparar el precio con el de mercado

Los "chollos" demasiado buenos para ser ciertos (precios muy bajos, ubicación inmejorable, calidades muy buenas...) pueden ser el gancho perfecto para captar nuestra atención.

Recomendaciones "Buenas prácticas del cibernauta"



!?

Excusas y problemas

Desconfiar si existe imposibilidad de enseñarnos el inmueble antes de alquilarlo o si nos obligan a continuar la comunicación fuera de la plataforma de anuncios.



No aceptar cualquier método pago

Los servicios de envío de dinero en efectivo, o transferencias a cuentas bancarias de países extranjeros, no nos permiten o dificultan la recuperación del dinero en caso de problemas o fraude.



Buscar en Google Maps

Podemos buscar la dirección del inmueble a través de Google Maps para comprobar si es real y se corresponde con la descripción del inmueble anunciado.



Enlaces relacionados

• Campaña concienciación sobre "Alquileres vacacionales"



Oficina
de Seguridad
del Internauta

RECOMENDACIONES para protegernos

05 | Falso soporte técnico

Aprendiendo a identificar fraudes online Pag. 07/12



"Estaba en mi ordenador trabajando en mi tesis, al mismo tiempo que navegaba por Internet buscando información en diversas fuentes. De pronto, una ventana apareció por pantalla indicando que mi ordenador estaba infectado, que no lo apagara y que llamara al número de soporte técnico que allí aparecía.

Tras hablar con el supuesto técnico, me explicó cómo instalar un programa para que él pudiese conectarse a mi ordenador y desinfectarlo de forma remota."



¿Cómo nos afectaría?

Los ciberdelincuentes podrían pedirnos dinero por hacer una **falsa reparación** del dispositivo o, incluso, **instalarnos programas maliciosos** en él para robar información privada y **realizar acciones maliciosas o ilegales** desde él.

Desinstalar las Apps

Desinstalar lo antes posible las aplicaciones que los estafadores te hayan pedido instalar.



Restablecer el dispositivo

Si hemos concedido acceso a los estafadores, consideremos la posibilidad de restablecer el dispositivo.



Actualizaciones de seguridad

Aplicar todas las actualizaciones de seguridad en cuanto estén disponibles.

Recomendaciones "Buenas prácticas del cibernauta"



Cambiar las credenciales

Cambiar las claves de acceso a nuestras aplicaciones y servicios.



Reportar el incidente

Si nos mintieron diciendo que eran el asistente oficial de un software, podremos reportarlo al proveedor original.



Llamar a nuestro Banco

Llamar a nuestro banco para cancelar los pagos al soporte técnico falso.



Instalar Apps originales

Instalar aplicaciones originales, solo desde las páginas webs oficiales.



Descarga Disponible
Google play



Descarga Disponible
App Store

Enlaces relacionados

Microsoft te ha llamado sin haberlo solicitado?

Mensajes fraudulentos, invitan llamar a un falso soporte técnico.

• Llamadas desde el falso soporte técnico.

• Servicio técnico falso, pero estafa real.



Oficina
de Seguridad
del Internauta

RECOMENDACIONES para protegernos

07 | Sextorsión

Aprendiendo a identificar fraudes online Pag. 09/12



“Mi hijo me comentó que, cuando estaba jugando en su ordenador, alguien le había enviado un mensaje al móvil amenazándolo con publicar en Internet unas fotos comprometedoras suyas si no pagaba una cantidad de dinero en menos de 24 horas.

En dicho mensaje se detallaba cómo habían obtenido sus fotos y cómo pensaban extorsionarle si no accedía a las peticiones.”



¿Cómo nos afectaría?

Este tipo de extorsión **consiste en chantajearnos con la publicación de fotos, vídeos o información íntima de nosotros, si no pagamos. En la mayoría de casos, no tienen nada, pero se sirven del miedo y el desconocimiento para engañarnos.**



No revelar información

Seremos cuidadosos con quién compartimos nuestra información personal, como fotos o vídeos.



Mantener la calma

Lo primero es no alarmarnos ya que puede tratarse de un engaño, y que no tengan los archivos que dicen tener.

Recomendaciones “Buenas prácticas del cibernauta”



Desconectar webcam y micrófono

Si no estamos utilizando la cámara u otros dispositivos de audio como el micrófono, es mejor desconectarlos. Tampoco es recomendable que permitan que cualquier app tengan acceso a la cámara del dispositivo.



No abrir archivos adjuntos

Si recibimos correos dudosos, no abriremos los archivos adjuntos, ya que podrán contener algún tipo de malware.



No enviar dinero

Realizar un pago no garantiza que no sigan extorsionándonos. Es más, estaremos favoreciendo este tipo de prácticas.

Enlaces relacionados

- ¿Buscas pareja por Internet? ¡Ten cuidado!
- Detectada una estafa a través de correo electrónico extorsionando con supuestas imágenes de contenido sexual
- Cuidado con las sesiones de fotos



Oficina de Seguridad del Internauta

RECOMENDACIONES para protegernos

08 | Perfiles falsos

Aprendiendo a identificar fraudes online Pag. 10/12



“Estaba chateando con mis amigos cuando de pronto, un chico al que no conocía me abrió chat y empezó a hablarme como si me conociese.

Cuando le pregunté, me dijo que me había conocido a través de una app de citas en la que no me había registrado nunca. Fui a comprobarlo y efectivamente, alguien había creado un perfil falso con mi información y datos de contacto.”



¿Cómo nos afectaría?

Los motivos que hay detrás de la creación de perfiles falsos son muy variados: **dañar nuestra reputación online**, extorsionarnos e incluso robarnos datos personales para cometer otras actividades fraudulentas. **Debemos tener cuidado con la información que publicamos en Internet.**



Ejercer derechos ARCO

Son los derechos de acceso, rectificación, cancelación y oposición de datos para la protección de nuestros datos personales.



Recopilar pruebas

Si nuestra identidad ha sido suplantada, deberemos recopilar todas las pruebas que podamos y reportar la situación a la web donde esté registrado el perfil falso.



Hacer “Egosurfing”

Una rápida búsqueda online sobre nosotros nos dirá si se han usado nuestros datos en alguna web que no conozcamos o utilizamos.

Recomendaciones “Buenas prácticas del cibernauta”



Mejorar la privacidad en la redes sociales

Toda red social pone a nuestra disposición la opción de decidir cuánta información queremos que se haga pública y a quienes queremos que llegue.



No aceptar peticiones de desconocidos

Si su descripción es escasa, no tiene fotos asociadas y además no le conocemos, ni tenemos conocidos en común, no le aceptaremos. Es posible que se trate de una cuenta falsa.



Ser selectivo

Agregaremos a usuarios que realmente conozcamos. Existen perfiles que solo buscan llamar la atención publicando bulos o creando polémica y discusiones entre los usuarios.

Enlaces relacionados

- Un doble en la Red
- Perfiles falsos en redes sociales, ¿cómo actuar?
- Qué hacer ante una suplantación de identidad
- ¡SOS! Alguien ha creado un perfil con mi foto



Oficina
de Seguridad
del Internauta

RECOMENDACIONES para protegernos



“Llevaba meses buscando comprar una videoconsola nueva a buen precio a través de una app de compraventa de productos, hasta que encontré un vendedor que la ofertaba a un precio muy bajo.

Me pidió que le pagara por adelantado haciendo una transferencia bancaria, él a continuación me enviaría la videoconsola. Sin embargo, tras efectuar el ingreso, el envío nunca llegó y cuando fui a preguntar al usuario, éste había desaparecido y su perfil ya no figuraba en la aplicación.”



¿Cómo nos afectaría?

El principal riesgo de los procesos de compraventa de productos es que el **vendedor o comprador nos engañe**, de tal manera que realicemos el **pago de un producto que nunca nos llegará** o que enviemos el nuestro y no recibamos el pago.



Observar el anuncio

Los estafadores suelen usar imágenes falsas sacadas de Internet u ofertar productos falsificados. Si dudamos, debemos pedir más imágenes o información al vendedor para cerciorarnos de que es real.



Sospechar de las excusas

Seguir la comunicación fuera de la plataforma, solicitud de dinero por adelantado y ofrecer pagar más cantidad de dinero por el producto sin ningún motivo son síntomas claros de que están intentando engañarnos.



Revisar comentarios

Siempre es útil revisar qué dicen otros usuarios sobre el vendedor. Si no tiene valoraciones o son pocas y negativas, desconfiemos.



No fiarse de ofertas muy agresivas

Desconfiar de productos con precios muy inferiores a los de mercado ya que son la excusa perfecta para engañarnos.

Recomendaciones “Buenas prácticas del cibernauta”



Revisar el perfil vendedor/comprador

Normalmente los perfiles de estafadores llevan muy poco tiempo creados, no tienen fotos reales ni datos de contacto verificados. Además, suelen tener urgencia en llevar a cabo la transacción. Si somos el vendedor, desconfiaremos de compradores con perfiles extraños o de países extranjeros que dicen tener urgencia en la compra bajo cualquier condición.



Aceptar métodos de pago seguros

Si vamos a pagar a distancia, acudir preferentemente a sistemas de pago, como son el pago contrareembolso, PayPal o Walla-pop Envíos, etc. que aseguren que recibimos el dinero o el producto.



Denunciar anuncio fraudulento

Si tenemos motivos para pensar que un anuncio es falso, se lo notificaremos a la plataforma que lo aloja para que pueda ser revisado y eliminado.

Enlaces relacionados

- Servicios de compraventa y subastas online
- ¿Qué son los sistemas de reputación?

Tarjetas prepago / monedero / virtuales



TARJETA PREPAGO

Tarjeta Virtual

Estas rebajas solicita tu Tarjeta Virtual y realiza compras seguras.

Solicítala →



Tarjeta digital BBVA

Cuando compras en línea **generas Puntos dobles**

Puedes **apagarla y prenderla** cuando necesites

Tiene un **CVV diferente** cada 5 mins

El número es **diferente** al de tu tarjeta física.

The app interface shows the BBVA digital card with the number 4152 3134 8895 9801 and valid until 07/26. Below the card, it shows the account balance: \$3,500.60 Disponible. The account is associated with BBVA. There are buttons for 'Apagar tarjeta' and 'Comprar con tarjeta digital'. Below the account information, there are buttons for 'Control de gastos' and 'Ver NIP'. The 'ULTIMOS MOVIMIENTOS' section shows two transactions: '15 de octubre Pago cuenta de tercero \$-5,000.00' and '14 de octubre Spei enviado azteca \$-1,500.00'.

Tarjetas prepago / monedero / virtuales



Productos

Cuentas, tarjetas, hipotecas...

Promociones

Hasta 250 € por tu nómina

Privilegios

IKEA, Naturgy, ADT Alarmas...

Acceso

e-Tarjeta

Tu tarjeta prepago para compras tanto físicas como online

Solicitar



¿Qué es CaixaBank Wallet¹ - MoneyToPay?

Una **tarjeta virtual vinculada a una de tus cuentas o tarjetas**, que podrás utilizar como método de pago para comprar por internet de forma sencilla y cómoda.



Solicitala ahora



Webs altamente fiables



Carrefour

Booking.com



PC
COMPONENTES

civitatis



Maquillalia
TU TIENDA ONLINE DE BELLEZA

Webs altamente fiables



Webs Dependende del vendedor, hay que leer las reseñas

